

国际信息工程先进技术译丛

电力线通信技术与实践

Power Line Communications in Practice

（法） Xavier Carcelle 著
刘斌 崔晓曼
方箭 刘颖 李长春 译





机械工业出版社
CHINA MACHINE PRESS

国际视野　科技前沿

国际信息工程先进技术译丛

《电力线通信技术与实践》
《现代通信原理》（原书第2版）
《认知无线电网络》
《高速数字系统的信号完整性和辐射发射》
《UMTS中的LTE：基于OFDMA和SC–FDMA的无线接入》
《生物医学工程学概论》（原书第2版）
《全面的功能验证：完整的工业流程》
《无线Mesh网络架构与协议》
《UMTS蜂窝系统的QoS与QoE管理》
《半导体制造与过程控制基础》
《WCDWA原理与开发设计》
《下一代移动系统：3G/B3G》
《IMS:IP多媒体概念和服务》（原书第2版）
《下一代无线系统与网络》
《深入浅出UMTS无线网络建模、
规划与自动优化：理论与实践》
《HSDPA/HSUPA技术与系统设计——第三代移动
通信系统宽带无线接入》
《无线传感器及元器件：网络、设计与应用》
《印制电路板——设计、制造、装配与测试》
《IPTV与网络视频：拓展广播电视的应用范围》
《多电压CMOS电路设计》
《微电子技术原理、设计与应用》
《蜂窝网络高级规划与优化2G/2.5G/3G/…向4G的演进》
《基于蜂窝系统的IMS——融合电信领域的VoIP演进》
《无线网络中的合作原理与应用》
《电生理学方法与仪器入门》
《移动电视：DVB-H、DMB、3G系统和富媒体应用》
《环境网络：支持下一代无线业务的多域协同网络》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3G CDMA网络》
《UMTS-HSDPA系统的TCP性能》
《宽带无线通信中的空时编码》
《数字图像处理》（原书第4版）
《基于4G系统的移动服务技术》
《吉规模集成电路互连工艺及设计》
《高性能微处理器电路设计》

上架指导：工业技术/电力线通信



● ISBN 978-7-111-33601-3
● 封面设计：马精明

定价：88.00元

地址：北京市百万庄大街22号
电话服务
社服务中心：(010)88361066
销售一部：(010)68326294
销售二部：(010)88379649
读者购书热线：(010)88379203

邮政编码：100037
网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com
封面无防伪标均为盗版

国际信息工程先进技术译丛

电力线通信技术与实践

（法）Xavier Carcelle 著
刘 斌 崔晓曼 方 箭 刘 颖 李长春 译
赵 媛 郑 娜 校



机 械 工 业 出 版 社

本书首先深入浅出地介绍了电力线通信技术的基本原理，包括电力线通信技术的结构、功能、安全性、帧结构等内容。然后图文并茂地从电力线应用实践的角度进行了全方位的阐述，包括电力线通信技术的设备情况、安装步骤、配置方法等内容。随后循循善诱地剖析了家庭环境、商业环境、社区环境下的电力线通信系统的拓扑结构、接入方法、应用方式以及有关注意事项和成本简析等方面的问题。最后介绍了混合 PLC 技术等内容。

本书特别适合电力线通信系统的研究开发、实验分析以及布设施工人员阅读参考，也适合无线电通信管理与标准政策制定人员在进行有关电力线通信技术规范化、标准化时进行参考，同时也可以作为相关院校师生的参考读物。

本书版权登记号：图字 01-2009-7837

图书在版编目（CIP）数据

电力线通信技术与实践/（法）卡塞勒著；刘斌等译．—北京：机械工业出版社，2011.3

（国际信息工程先进技术译丛）

ISBN 978-7-111-33601-3

Ⅰ.①电… Ⅱ.①卡…②刘… Ⅲ.①电力线载波通信系统 Ⅳ.①TM73

中国版本图书馆 CIP 数据核字（2011）第 033569 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）

策划编辑：朱 林 责任编辑：朱 林 版式设计：霍永明

责任校对：樊钟英 封面设计：马精明 责任印制：杨 曦

北京中兴印刷有限公司印刷

2011 年 6 月第 1 版第 1 次印刷

169mm×239mm · 19 印张 · 381 千字

0 001—3 000 册

标准书号：ISBN 978-7-111-33601-3

定价：88.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务 网络服务

社服务中心：(010)88361066 门户网：http://www.cmpbook.com

销售一部：(010)68326294 教材网：http://www.cmpedu.com

销售二部：(010)88379649

读者购书热线：(010)88379203 封面无防伪标均为盗版

序 言

电力线通信（Power Line Communication）技术距离我们并不久远，早在20世纪50年代就有在10kV线路上使用窄带载波技术的先例。20世纪80年代末期，我国也曾使用小型化的集成电路农电载波机实现点对点的通信。随着通信技术的不断发展，高速宽带电力线通信技术的研究与应用正在悄然兴起。一时间，电力线通信技术出现了多个不同的名字，例如BPL（Broadband over Power Line）、PLT（Power Line Telecommunication）技术等。进入21世纪，人们再一次将目光集中到电力线通信技术，不断提升电力线通信技术的物理层传输速率，加强抗干扰性能的研究工作等。

近几年来，人们在研究电力线通信技术的同时，也发现了电力线通信系统可能辐射出不同频段的电磁波，因此国际电信联盟无线电通信部门研究了80MHz以下的高速宽带电力线通信的辐射对其他无线电通信系统可能产生的影响，并正在着手研究可能工作在VHF频段的电力线通信系统的辐射影响情况。

更好地从包括监管角度在内的多个方面研究电力线通信技术需要更多地了解电力线通信系统的实际应用情况。不过，目前国内关于这方面的书籍相对较少，特别是关于电力线在不同场景的拓扑结构、接入方式、设备配置等方面的书籍和公开文献也不太容易找到。相信本书的出版对我国有关领域的技术人员和相关院校师生进一步多角度研究电力线通信技术、对有关标准化研究人员科学合理地研究和制定相应的技术和管理标准等将起到十分积极的作用。

薛永刚

2011年仲春于北京

译 者 序

近年来电力线通信（Power Line Communications，PLC）技术发展迅速，特别是新一代高速电力线通信技术的异军突起，使得家庭高速数据传输等需求通过电力线得以实现。由于电力线通信技术不仅涉及通信技术本身，还受到电力网络系统的组成和系统特点等方面因素的限制和影响，因此在研究、开发以及布设电力线通信系统的过程中，技术人员、管理人员以及标准政策制定人员等都亟需一本集电力线通信技术基础、系统安装、相关标准以及在家庭、商业、社区等环境下的系统调试指导于一体的技术参考书。

本书介绍了电力线通信技术的基本原理，展示了电力线通信系统的主要设备，给出了典型应用环境下（家庭、商业、社区等）的电力线系统配置与布设的技术要求和注意事项等。读者阅读本书之后，可以清楚地理解电力线通信技术的基本原理、设备构成及其配置要求，并对其研究、开发以及标准规定的编写等工作有所指导与帮助。

本书由刘斌、崔晓曼、方箭、刘颖、李长春承担主要翻译工作，参加翻译工作的还有赵媛，郑娜等。李长春、赵媛、郑娜还对本书的第一译稿进行了数次校对和补遗。此外，陈怡、王爱举等完成了本书部分文字和图表的翻译等工作。全书由刘斌负责统稿审定。

需要说明的是，本书是译者在尽量忠实于原书的基础上翻译的，为保持原书特色，书中部分图形符号和文字符号并未按国家标准做修改，请读者注意。本书的内容仅代表了作者个人的观点和见解，并不代表机械工业出版社和译者的观点。

本书的出版得到了各位译校者、机械工业出版社有关同志的大力支持。国家无线电监测中心薛永刚副主任也在百忙之中欣然为本书致序。在此鸣谢为本书付出辛勤劳动的各位译校者，同时对为本书提供过帮助的人员一并表示诚挚的谢意。

由于译者水平有限，在翻译、整理本书的过程中一定还有很多不足，如有不准确之处，恳请读者批评指正。

译 者
2011 年 4 月

中文版前言

自第一台 PLC（Power Line Communications，即电力线通信）设备于 2000 年问世以来，PLC 技术以提供最佳的性能为宗旨，一直在稳步发展、前进。如今，PLC 技术已经成熟，可以与其他相应的局域网技术相媲美，并且部署起来更加便捷。众多通信专家的观点以及本人 2006 年以来的实践都充分表明，PLC 技术已经从鲜为人知转变为广为人知，得到了极大的重视，并在众多普通的家庭中得以应用。

PLC 可以更为便利地在整个楼宇中传输任何类型的数据，其中也包括众多 ISP 新近提供的基于 IP 服务的视频信息数据。作为 ISP 而言，他们更乐于通过使用以太网的接口与其他网络终端实现通信，从而达到服务最大 IP 用户数量的目的。

当前，IEEE 已经通过了 IEEE 1901 系列下的标准，并且逾 4000 万台 PLC 设备使用了这一专门标准。这一标准包含网络和安全架构方面所应遵守的规定，并且包含了家庭环境下的电磁兼容（EMC）方面的要求。该技术与业余无线电的干扰问题，在共同使用一部分子带频段技术后已得到解决。PLC 与业余无线电技术之间的干扰问题正在通过一种对普通子载波频率上进行“开槽”的智能技术来解决。

相信在不远的将来，随着 PLC 接口更为广泛的集成化（集成到 Wi-Fi、以太网、有线电视线缆之中等），PLC 设备市场将会继续向前发展，从而实现网络工程师和电信公司目标，即大型的 PLC 公司融合至 Wi-Fi 公司之中。

Xavier Carcelle

2010 年 12 月

原书前言

自从2000年初出现第一个电力线通信（PLC）设备，电力线通信技术便一直稳步发展，其发展目标就是实现最佳的性能。如今PLC技术已经成熟，其性能已经可以与其他局域网技术相提并论，不过PLC技术的另一个优势便是其开发与部署更加简单。

PLC技术可以使得在整栋楼里广播各类格式的数据变得更为简单，这其中便包括通过近年来ISP所提供的基于IP的视频数据业务（Video over IP）。ISP期望其终端能够通过以太网接口与其他终端和因特网相连接，并期望能够容纳最大IP应用数量。

当前IEEE关于PLC的标准不多，因此人们往往将Home Plug技术作为实际的技术标准，因为当本书出版时，世界上正在使用的PLC设备的数量已经达到了1500万台左右。IEEE的一个工作组即将完成第一个高性能的电力线通信技术标准的草案，该草案能够确保并且符合家庭环境下的电磁兼容的要求。PLC系统对业余无线电系统（Ham Radio）的干扰问题已经得到了解决，解决方案是在两个系统共享的频段中对PLC系统的信号进行智能的开槽（Notching）。

电力线通信技术的设备及其集成接口（与Wi-Fi、以太网、有线电视等的接口）市场将来会不断增长，从而既满足网络工程师的需求也满足电信公司的目标。

本书的结构

本书从理论到实际应用展示了PLC技术的各个方面，此外，本书还可以作为个人、专业人员以及有关企业使用PLC网络时的安装指导资料。

作者以及本书的其他撰写者在本书的编写过程中将最富教学意义的内容融入其中，这样做是为了使得未来的安装者和用户能够对与电力网络和计算机网络相关的PLC技术驾轻就熟。本书通过大量图表对不同的研究情况进行了说明，展示了工程师们在部署PLC网络时出现的问题和解决方法等。

本书共13章，分为两大部分。

● 第1章：概述。第1章介绍了PLC技术的历史以及当前当今不同组织（联盟和工业组织等）所开展的引导PLC技术向前发展的工作。

● 第1部分：PLC原理。这一部分将集中分析与PLC相关的电力和计算机网络技术的特征，以及与PLC技术相关的不同功能，这些技术和功能使得PLC能够将数据流通过各种不同的方式传输给最终用户。

● 第 2 章：PLC 的结构。本章通过着重分析电力网络与电信领域通用模型之间的关系，描述了电力网络的属性。

● 第 3 章：PLC 的功能。本章列举了在电力网络中实现最佳数据交互的一整套功能。

● 第 4 章：PLC 的安全。虽然 PLC 不用面临与 Wi-Fi 网络类似的安全问题，但是 PLC 必须建立一些安全标准。

● 第 5 章：PLC 的数据帧结构。本章介绍了在电力网络中传输的完整的数据帧结构。

● 第 2 部分：PLC 的实际应用。这一部分内容涵盖了所有的 PLC 实际应用，即从家庭用户或专业用户场景，到满足城市需要的因特网接入场景。

● 第 6 章：PLC 的应用。当前，ISP 所提供的因特网接入囊括了越来越多的应用（例如声音、数据、图像、高清视频流等），这些应用在数据吞吐量和安全等方面有着较好的表现。本章说明了 PLC 网络如何满足这些需求。

● 第 7 章：PLC 的设备。PLC 设备的正确选择需要对不同 PLC 所使用设备的功能有较好的了解，比如网关、过滤器、中继器、注入器以及其他网络配件。本章介绍了不同安装条件下不同功能所对应的标准的选取等内容。

● 第 8 章：PLC 的安装。在安装前正确地设置 PLC 设备是非常重要的。本章介绍通过对电力网络中 PLC 设备位置的优化，解决经常出现的安装问题。

● 第 9 章：PLC 的配置。本章描述了在不同平台下（Windows、Linux 和 FreeBSD）以及不同类型的 PLC 技术条件下的配置步骤。

● 第 10 章：PLC 在家庭中的应用。想在家中安装 PLC 网络的人们在本章中可以找到他们所需要的所有信息，这些信息将指引他们做出正确的选择。另外，本章还提供了配置和安装等方面的建议。

● 第 11 章：PLC 在商业中的应用。从 SOHO 到大型的多个厂房的工业公司，专业人士在本章中都能够找到详尽的内容，指导其采用不同的步骤来优化电力网络，使其作为局域网（LAN）的骨干网。

● 第 12 章：PLC 在社区中的应用。本章重点分析了偏远地区的社区所面临的因特网接入问题，并给出了通过使用公共电力网络接入因特网这一项目的管理中所需要遵循的构架原则和解决方案。

● 第 13 章：混合 PLC。这是本书的最后一章。本章描述了 PLC 与其他网络技术的不同，并展示了在局域网中将 PLC、Wi-Fi、以太网、有线电视和 PSTN 来建立一个混合结构的优点所在。

谨以此献给 *Yves*，*Françoise*

致　　谢

我想首先感谢 Artech 的人们，即我的主编：Simon Pluntre 以及 Judi Stone，他们一直陪伴并支持着本书的编写。

非常感谢 Michel Goldberg，我认为他是在 PLC 网络标准化领域的最好的专家之一。Michel 审查了全书的内容，确保了第 1 部分的质量，为完成这样一本书贡献了很多的专业知识。

同样感谢 Florian Fainelli 和 Nicolas Thill，他们是我所认识的最好的 Linux 开发者。是他们在 OpenWRT 项目中 Wi-Fi 的专业知识帮助我了解 PLC 网络的结构控制。

毫无疑问，我也要感谢 PLC 设备供应商的同事，即 DEVOLO 的 Werner Fehn、Intellon 的 Andy Barnes、Current 的 Terry Bernstain 以及 LEA 的 Frederic Guiot。

图例的制作应当归功于 Marie-Helene Phuong，基于我的原图，她的图形设计是令人难以置信的。她的工作将绝对能够帮助读者完全理解 PLC 网络的原理。

目　录

第1章 概 述

电力线通信（Power Line Communications，PLC），是一种通过中低电压电力网络来提供通信服务的技术。

尽管PLC在它首次应用时，是从一个频率范围较低级别开始，然而如今的PLC也越来越多地在高频段中得以应用，这一应用也常被称作宽带电力线（Broadband Power Line，BPL）。

很长一段时间以来，电力网络也用于发电和配电领域低速的网络监控和远程控制。

如今，发电和配电都不能忽视标准化的问题。非常有趣的是，电力网络的部署、它们之间的互连以及不断增长的电器数量已经造就了第一个网络标准化实体，这就是国际电工委员会（International Electrotechnical Commission，IEC）。

1.1 PLC技术

PLC技术背后的原理并不是最近才出现的。早在1838年，英国人Edward Davy就提出了一套解决方案，通过伦敦和利物浦之间有线电报系统远程测量电池的电压。1897年，他提交了第一个专利（不列颠专利第24833号），专利的内容就是通过电力线的通信，实现电力网络电能表远程测量的技术。

1950年，第一个PLC系统问世，它被部署在中压和低压的电网中，这个系统也常被称作Ripple Control，载波频率在100Hz～1kHz之间。当时非常需要通过控制信号建立单向通信，从而实现远程控制公共路灯或者调整价目表。第一个工业化PLC系统于1960年在法国问世，被称作Pulsadis，该系统涉及的电力能量接近100kVA。

随后，第一个CENELEC[⊖]频段的PLC系统就问世了，该系统的工作频率覆盖了3～148.5kHz，并且可以在低压电网中双向通信。例如对远程电表读取以及一大批和家庭自动化领域有关的应用（入侵报警、火警检测、气体泄漏检测）等。由于该系统涉及的电力能量已经降低至大约100mW这一数量级，因此，PLC系统所需要注入的功率相应地减少了许多。

1945年，第二次世界大战结束之后，电力线载波（Power Line Carriers）一词

⊖ CENELEC是欧洲电工技术标准化委员会的法文名称。——译者注

经常被缩写为PLC。在那个年代，众多电话线和电力线已遭损坏，但是残存的电力线数量要比电话线多出许多。出于通信的目的，系统往往设计成通过高压或中压电力线进行数据传输，传输的方式就是模仿已经在电力线上付诸使用的远程电表读数抄写系统的工作原理。

图1.1说明了自20世纪90年代以来PLC发展变化的情况。

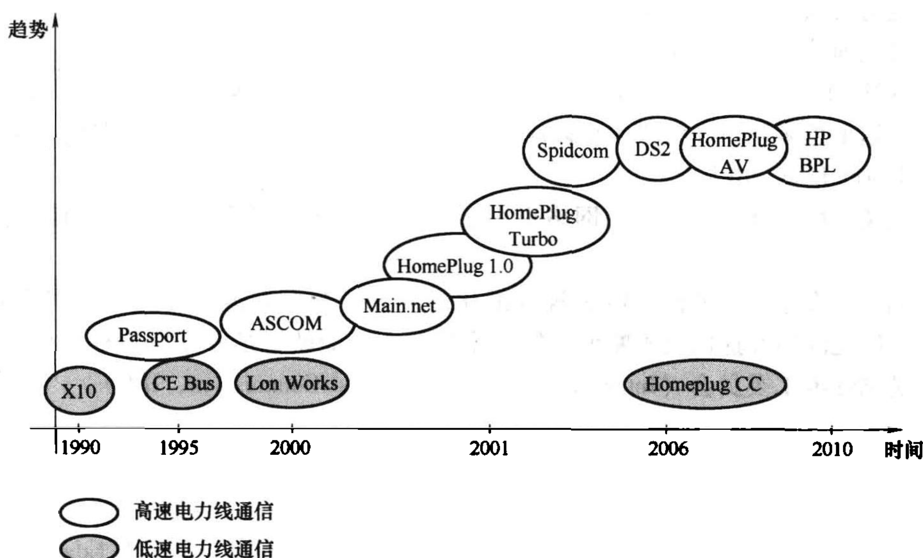


图1.1 低速和高速PLC技术

1.1.1 标准化组织

本节将展示大量的标准化机构，同时我们也将会澄清“标准”和“规范”的概念。

“标准”一词涵盖了若干种类型的文件。

尽管在英文中，人们大都将“准则（norm）”和“标准（standard）”统称为“标准”，但是它们两者之间是不尽相同的。“准则”是来自国际化机构的一个文件，譬如说ISO（国际标准化组织）。有时“准则”也被称作“法定标准（standard de jure）”。在接下来的章节中，我们称这些准则为“标准”。

“标准”是源自于国家级机构的文件，比如美国的IEEE，或者源自于国家间的团体组织，比如欧洲的ETSI（欧洲电信标准协会）。为了能够区别，我们有时将其称作“事实标准（de facto standard）”。我们将此类标准称作“规范（specification）”。

为了能够简要地描述一个“标准”能够完成的内容，我们这里不妨引用ISO

的定义：“标准是任何一个为重复性活动设计的、经由普遍被认可的一个标准化机构所批准并由各方共同遵守的文件。”这是大多数人意见的体现。

考虑到地域范围的不同，标准化工作可能是国际化的，或者首先从一个区域化的层面开始实施。

在欧洲，标准化工作在欧洲国家内部、欧洲和国际3个层面展开。每一个标准化委员会分别负责一个或者几个标准化领域。

目前，有3个不同的组织涵盖了全部学科领域，分别是国际电工委员会（IEC）、国际标准化组织（ISO）和国际电信联盟（ITU）。

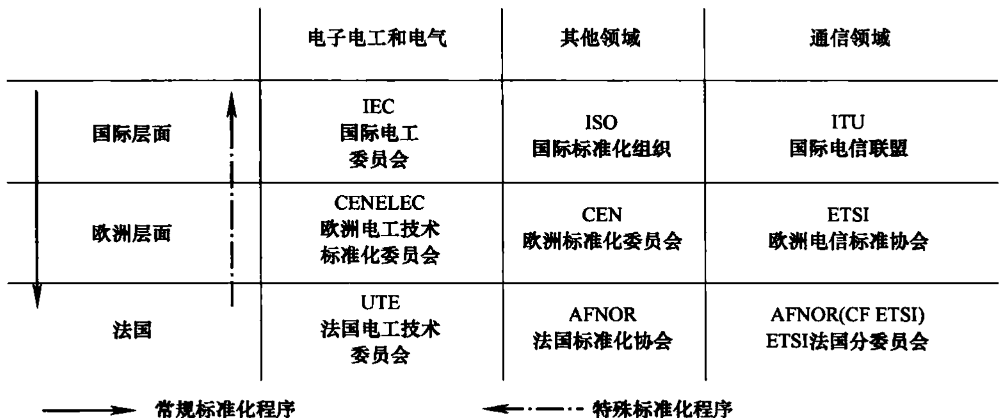
国际电工委员会（IEC）和欧洲电工技术标准化委员会（CENELEC）负责电子工程领域，欧洲电信标准协会（ETSI）负责通信领域。

国际标准化组织（ISO）和欧洲标准化委员会（CEN）负责其他领域的标准化活动。

在欧洲，协调一致的国际标准的条款将在所谓新方式的大背景下得以应用，这种新的方式为：按照欧盟委员会与相关标准机构之间达成的一般性方法，在欧盟委员会授权的框架下与成员国协商后，使用欧洲指令的形式明确欧洲的国际性标准的应用。

图1.2说明了每一个标准化委员会所负责的PLC技术的活动内容。

必须指出，图1.2中的区域性标准的各个层面（这里指欧洲）在世界其他地区似乎并不是那样明确存在（亚洲、东方等）。



	电子电工和电气	其他领域	通信领域
国际层面	IEC 国际电工 委员会	ISO 国际标准化组织	ITU 国际电信联盟
欧洲层面	CENELEC 欧洲电工技术 标准化委员会	CEN 欧洲标准化委员会	ETSI 欧洲电信标准协会
法国	UTE 法国电工技术 委员会	AFNOR 法国标准化协会	AFNOR(CF ETSI) ETSI法国分委员会

图1.2 负责PLC技术的标准化组织

在欧洲国家，自从欧盟委员会将国际标准、规范定为CE标识的参考后，这一基本的标准化层面结构就显得尤为重要了。

为了在广义上更好地理解国际标准实施的机制，这里将欧洲标准化组织的情况

与美国标准化组织的情况进行比较。

如果我们看一下《美国标准系统概览》（美国国家标准学会，第2版，2007年7月），就会知道美国标准化机制的与众不同。一般地，一个国家会指定一个组织为主要的标准研究与开发单位，并且这个组织（如果不是政府的某个部分）和政府关系很密切，但是在美国，大量的组织（政府的或是非政府的）便构成了美国标准化体系。

在美国，标准以及规定主要分为两个大类，分别是强制性标准和自愿性标准。强制性标准是由政府设立的，它们可以是关于政府采购的标准，也可以是关于政府监管的标准。采购标准列出了政府供应商必须满足的要求；监管标准可以就健康、安全、环境以及其他判定准则等作出规范。

对于自愿性标准，在美国，自愿性标准研制体系之所以被称作“自愿”是出于两个理由：第一，参与这个体系是自愿的；第二，标准通常是为了主动使用而研制的。自愿性标准由感兴趣的利益相关者参与制定并达成一致，这些利益相关者包括生产者、使用者、消费者、政府和学术界代表。

在美国，自愿性和强制性的区别不是非常明确。通常政府标准的制定者会在其规定中引用由私人开发的标准，这样做也就相当于由政府给这个私人标准予以官方支持。以建筑法规为例，它里面就参考了由自愿性标准组织开发的数以百计的标准。建筑法规是属于政府范畴的，因此所参考的这些标准具有法律效力，并且相关管理机构必须遵守，这些机构有联邦航空管理局、环境保护局、食品药品管理局等。住房和城市发展部门也会参考至少数以百计的被一致认可的自愿性标准作为自己有关规范的替代标准。这些用来参考的若干标准，一旦在政府管理规定中使用，它们也同样会具有法律效力。《美国国家技术转移与进步的法案》（公共法104-113）提倡政府机构只要条件允许就可以使用私人研制的标准。这一做法正在不断增加，并且为纳税人节约了原来的标准研制体系中重复劳动所导致的数百万美元的开支。

1.1.2 有哪些类型的标准

根据研制和使用所需要达成共识的程度不同，标准至少可以分为4种。《标准化手册》（美国实验材料学会ASTM，2006年4月出版）里对标准进行了如下分类：

公司标准（Company Standard）：一个组织机构中员工之间的共识。

联盟标准（Consortium Standard）：一小群组织机构之间的共识。由具有相同意向的公司组成一个联盟，这个联盟所从事的活动将超过任何单一成员公司的资源能力范围。美国汽车研究委员会的战略标准董事会就是联盟标准的一个例子。该董事会反映出美国汽车研究委员会所承担的与竞争力相关的标准管理

问题。

行业标准（Industrial Standard）：它是指在一个协会（association）或专业社团（professional society）内的多家公司之间的共识。比如，由多个不同的石油公司组成的贸易协会，即美国石油协会（API）所开发的标准，就属于行业标准。

政府标准（Government Standard）：政府标准可以反映出不同程度的共识。有些政府标准是政府机构中的个人撰写的，然而更多标准是由一些专门机构研制的，然后作为强制性标准被采纳。纳入到联邦法规中的由环境保护机构（EPA）或职业安全和健康管理局（OSHA）所负责的相关标准就是政府标准的一个例子。

根据ISO，国际标准是“一个用于重复性活动的，由一个被认可的标准机构批准的，并可向公众公开的文件。”

法国标准化协会（AFNOR）通过以下方式完善了此定义：“国际标准是一个参考性信息，它源自深思熟虑后作出的集体性决定，是用于解决重复性问题的行为基础。”

我们必须指出它与法规的关系：国际标准只定义了方法和规则；因此它不是强制的，与法律法规并不相同。

正如前面所提到的，欧洲的标准管理框架是建立在新方案指令上的。这些指令列出了产品必须满足的基本要求。协调统一后的欧洲标准只要满足了各自要求，就应当能够符合这些基本要求。

协调统一国际标准的重要性可以通过CE标志来说明。有了这个标志，产品就可以自由地在欧洲流通。同时，它也是制造商的一个声明，即表明它的产品符合欧洲指令关于该类产品的基本要求。

PLC设备必须满足电磁兼容性（EMC）和低电压（LV）指令中的基本要求。

就PLC来说，应当将PLC产品与PLC系统、网络的工作分开来讲。截至目前，关于PLC产品的研究工作修订了CISPR 22标准，这是一个国际出版物。然而与PLC网络相关的标准研究工作仅在欧洲展开，并且研究工作由欧洲电工技术化标准化委员会/欧洲电信标准协会（CENELEC/ETSI）的联合工作组承担。此国际标准的目的不是限制有线网络的发展，而是限制其干扰辐射。

经过5年的努力，人们试图达成共识，但是最后发现，对有线网络的辐射制定限值几乎是不可能的，于是最终放弃了研制PLC网络国际标准的想法，取而代之的是关注产品本身的国际标准。

与此同时，在全体PLC界的要求下，2005年4月欧盟委员会公布了一个建议书，该建议书规定了PLC的法律框架。建议书指出，成员国应当取消对PLC网络开发的任何障碍；作为回报，安装商、设备生产商和网络接入供应商必须承诺遵守EMC指令的要求；如果经证实，在许可的频段上出现干扰事件，则必须使用可能的任何远程干扰缓解手段。

2005年6月欧洲建议书节选

1）成员国应将以下条件和原则用于制定公开可行的宽带电力线通信系统的有关规定。

2）在不影响第3～第5点的前提下，成员国应消除（特别是来自公用事业公司的）对宽带电力线通信系统部署和电子通信服务条款中任何不合理的规定的障碍。

3）在用于规范电力线通信系统的标准在89/336EEC指令下得以协调统一之前，成员国应遵照此指令，即电力线通信系统是：

① 由符合指令的设备构成并且按其设计用途使用。

② 根据符合指令的基本需求所定义的良好的工程操作来安装和运行。

关于良好工程操作的文件应该本着监督检查的目的，在系统运行的整个时间段内，由相应的国家主管部门来制定。

4）如果电力线通信系统出现不能由各相关方面解决的有害干扰，成员国的主管部门应该索取系统是否符合规定的证据，并在适当的情况下开始进行评估。

5）如果评估得出电力线通信系统不符合规章制度的结果，相关主管部门应该使用适当非歧视性和透明的强制手段来确保PLC符合规章制度。

6）如果评估得出电力线通信系统符合规定，但仍然存在干扰，成员国的主管当局应该考虑根据89/336EEC指令第6条，采取适当非歧视性和透明的特殊手段。

7）成员国应当按时向通信委员会汇报在其地区的电力线通信系统的部署和操作情况。此报告应该包括干扰层面的相关数据（包括测量数据、相关注入信号强度和其他可供制定统一的欧洲标准的数据、干扰问题以及与电力线通信系统有关的强制措施），第一份报告在2005年12月31日前已提交。

8）这项建议已经寄往成员国。该项建议于布鲁塞尔完成，并于2005年5月6日至欧盟委员会，Viviane REDING，以及欧盟成员国。

在欧洲电工技术标准化委员会（CENELEC），PLC的导则被下列技术委员会（TC）和子委员会（SC）所遵守：

- TC 205，“家庭和建筑电子系统（HBES）”；
- SC 205 A，“电力线通信系统”；
- TC 210，“电磁兼容（EMC）”国际无线电干扰特别委员会（CISPR旗下）。

SC 205是一个关于“产品”的子委员会，旨在为“使用低电压电线或房屋布线在3kHz～30MHz之间频段上实施通信的系统制定一个协调统一的国际标准”，这个任务也包括为低电压电网条件下信号传输的频率分配。

遵照国际电工委员会（IEC）非重复的工作准则，关于PLC产品的国际标准研

制定工作或多或少地需要在这个子委员会中进行研究。

图1.3显示了各方（主体、联盟、国家、欧盟委员会等）与欧洲PLC国际和国内标准相关的工作之间的联系，特别是国际电工委员会（IEC）、欧洲电工技术标准化委员会（CENELEC）以及欧洲电信标准协会（ETSI）。

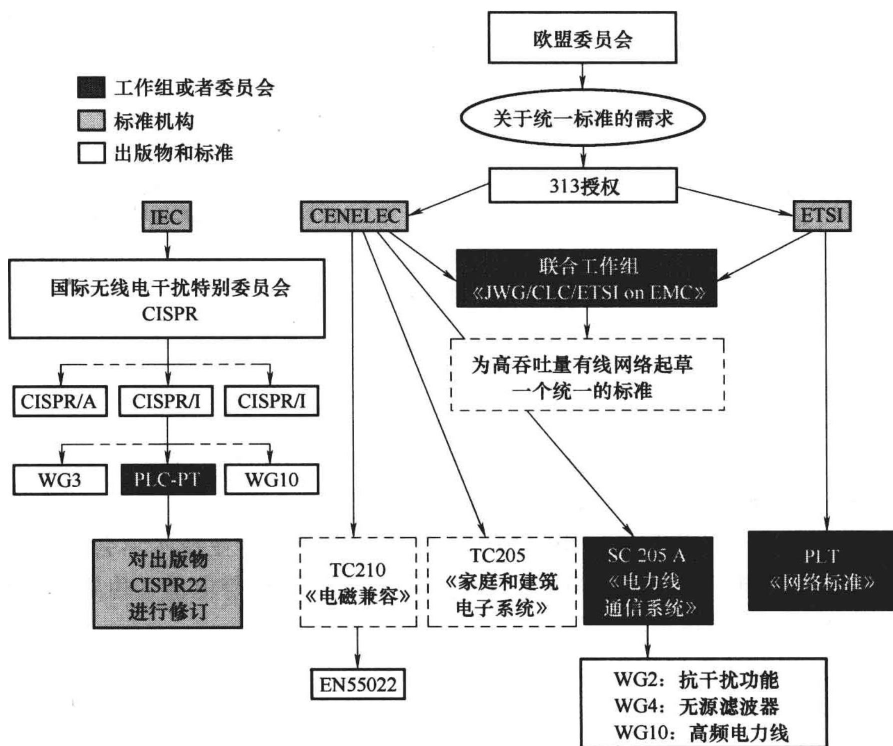


图1.3　与PLC标准化工作相关的组织或机构

1.1.3　联盟与协会（学会）

除了上述组织与机构外，某些协会和联盟在电力线通信的预标准化，甚至于标准化工作中也发挥着重要的作用；其中主要的3个联盟和协会是HomePlug联盟、IEEE以及Opera联盟。在欧洲，从历史上看，所有推动电力线通信的活动均由PUA和PLC论坛发起。

图1.4显示了PLC的预标准化中涉及的每一个机构的角色。

HomePlug联盟

HomePlug联盟集团的制造商既涵盖了电力线通信技术领域，也涵盖了相应的服务领域。其目的是制定HomePlug规范（HomePlug 1.0、HomePlug AV和Home-

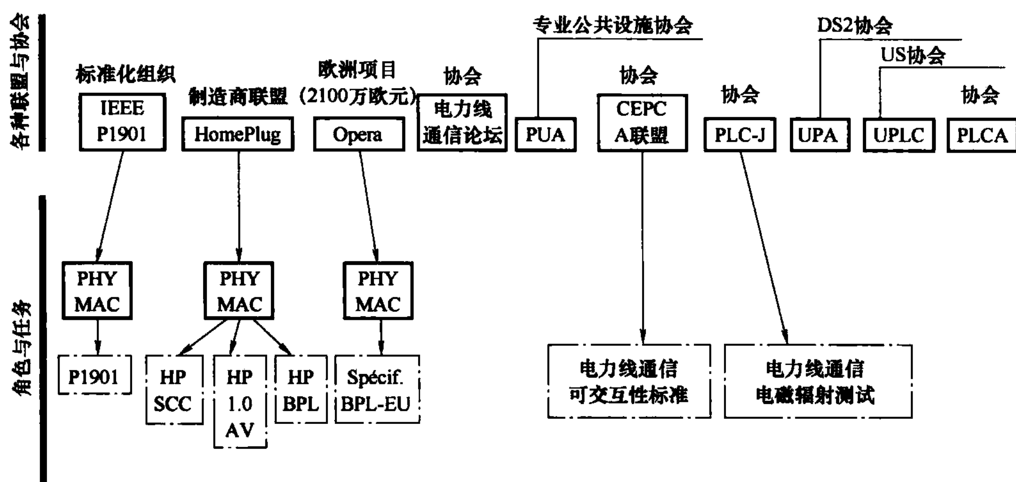


图 1.4　与电力线通信有关的联盟与协会（学会）

Plug BPL）。

目前，仅完成了 HomePlug 1.0 规范，并已经在众多市场产品中得到执行。

IEEE （美国电气电子工程师学会）

IEEE 作为一个非赢利性组织，是世界上最大的国际专业技术学会和主要的权威机构之一。该组织所涉及的领域包括航空系统、计算机与电信、生物医学技术、电能和消费类电子产品等。

IEEE 为其成员不仅提供信息与资源，而且也提供技术与专业服务。为了激发从事该技术领域相关工作的兴趣，IEEE 还为其遍布全球的学生会员提供服务。

IEEE 的另一个主要方面则由潜在客户、个人和公司组织等组成，他们购买 IEEE 的产品并参加 IEEE 的会议与专题研讨会。

Opera 联盟

Opera 联盟共有 36 个成员，来自欧盟不同国家和以色列。参与电力线通信技术研究的所有组织和协会均加入了该联盟，这些组织和协会涵盖了从公共服务提供商至电信运营商，直至芯片组制造商、调制解调器生产商、咨询机构和大学等。

丰富各异的人员结构与技术结构，对于实现该联盟的目标起着至关重要的作用。

Opera 联盟的战略目标定位于“通过最广泛的基础设施——电力线通信网络，为所有的欧洲居民提供高速接入服务。”为了实现这一目标，Opera 联盟展开了丰富的研究与开发工作，并在欧洲范围内组织演示与推广工作，致力于克服任何残余障碍，使得电力线通信运营商可以以极具竞争优势的价格为每一位欧洲居民提供高速接入服务。

Opera 联盟的主要任务是：

- 总体提高低、中电压 PLC 系统（速度、简单部署等）；
- 开发 PLC 网络接入主干网的最佳解决方案；
- PLC 系统标准化。

PUA （PLC 公共事业联盟）

PUA 是于 2002 年 1 月 21 日在马德里组建的联盟，它致力于向 10 亿欧洲用户提供公共服务，目前有以下成员：

- 法国电力公司（EDF），法国
- 恩德萨（Endesa）网络工厂，西班牙
- 意大利国家电力公司（Enel），意大利
- Iberdrola，西班牙
- 葡萄牙电力（EDP），葡萄牙
- EEF，瑞士
- Fenosa 联盟，西班牙

PLC 论坛

PLC 论坛是于 2000 年早期由两个协会合并组成的国际组织，与其他机构一同开展与 PLC 有关工作的活动。

1.2 走向标准化的 PLC 技术

任何标准化都是缓慢的过程。由于标准的制定需要工作组所有成员达成共识，因此标准化的缓慢推进也不足为奇。

虽然这个办法在大多数工业领域被证明是有效的，但是或许不太适合信息技术领域，因为信息技术领域的国家标准，其基本目的应该是以满足客户的紧急需求为主。

1.2.1 IEEE 未来标准

2005 年 6 月初，IEEE 指导委员会批准了“IEEE P1901 电力线网络宽带通信标准草案：MAC 和物理层技术规范”的电力线通信标准的起草工作。

该标准将可以适用于高吞吐量电力线通信设备（物理层比特率在 100Mbit/s 以上），适用频率范围不超过 100MHz，并可以解决接入技术和内部网络等方面的相关需求。此外，该标准也应该能够定义不同电力线通信设备之间的共存与互操作机制、所提供的服务的质量，以及数据保密性等。与电力线通信有关的各方基本上都参与了该项目，特别是表 1.1 中所列出的相关方。

1.2.2 未来互操作性标准

互操作性标准正力图解决家用、专业以及公用电力网络等领域出现的多种电力线通信规范与技术之间的交互问题。

由于作为通信介质的电网是共享的，因此，这些不同技术以共同的频带共存于电力电缆之上。IEEE 和 CEPCA（消费性电子电力线通信联盟）内涉及电力线通信的各相关方协同工作，力图使这些技术之间具备互操作性。未来型标准详见第 13 章，该章还对电力线通信网络进行了展望。

1.3 PLC 的优势和劣势

像任何一个有望获得成功的系统一样，与其同类技术相比，电力线通信技术既有优点，又有不足之处。该技术的不足之处之中，有一个是与室外（周边）和接入网络有关产品的相对不成熟性。大数据吞吐量时，主要是涉及电磁兼容性和辐射限制符合性等方面的问题。

表 1.1 IEEE 中与电力线通信标准化有关的主要相关方

南非先进通信网络公司
安便公司
Arkados 有限公司
消费者电子电力通信联盟管理署
科胜讯系统公司
Corinex 通信公司
Current 技术公司
DS2
杜克电力公司
Earthlink 公司
HomePlug 电力线联盟
国际商业机器公司
国际带宽电气通信（IBEC）公司
Intel 公司
Intellon 公司
伊藤忠商事株式会社
三菱电气公司
三菱材料有限公司
松下电器产业株式会社
先锋公司
PUA
RadioShack 公司

（续）

施耐德电气电力线通信公司
SiConnect 公司
索尼公司
速比特技术有限公司
住友电气工业有限公司
德州仪器公司
东京电力公司
东洋网络系统有限公司
通用电力线协会
Xeline 公司
雅马哈公司

电力线通信技术的优点主要有：

1）可以利用现有电力网络，且相关电力网络可能覆盖被考虑的整个国家；

2）部署快速；

3）无需额外布线；

4）可以采用功能强大、可靠的加密方法。

第 1 部分

PLC 原理

本书这一部分将主要涉及 HomePlug 规范（HomePlug 规范由与其同名的行业联盟所制定），并主要关注以下两个方面：与电力线介质上的数据传输密切相关的物理层；以及用于明确架构与工作机制、使该网络上的数据在可能的最佳条件下进行传输的数据链路层。

HomePlug 1.0 发布之后，已经开发了两个后续版本，进一步提高了传输速率、安全性和服务质量等。

为了提高数据传输性能，物理层使用了最优化的编码、调制和纠错技术，实现了设备之间极佳的连接性和理想的传输速率。HomePlug 1.0、Turbo 和 AV 相应的传输速率分别为 14Mbit/s、85Mbit/s 和 200Mbit/s，使得 PLC 技术完全可以与以太网和 Wi-Fi 网络相竞争。

数据链路层实现了一组技术，为以 IP 包的形式高性能地传输数据提供了极佳的条件。定义该层的网络接入技术对网络的性能起着决定性作用。

后续版本的 HomePlug 规范进一步提高了该层的性能。采用了时分多址接入（TDMA）技术，优化了服务质量；通过层次化结构的数据帧，进一步细化了 PLC 设备网络架构的管理。对于实时应用，例如就音频或者视频应用来说，服务质量是数据传输的一个关键因素。

接入 PLC 的物理介质的难度极大，这进一步提高了 PLC 的抗攻击功能。因此，与 Wi-Fi 相比，PLC 技术具备更高的安全等级。对电力线介质所传输的数据帧进行 DES 和 AES 加密处理、使用网络完整性技术对接入 PLC 网络的设备进行授权管理，更进一步增强了这种抗攻击能力。

第2章　结　　构

电力线通信（Power Line Communications，PLC），是利用电力线传输数据的一种网络技术的统称，它是深入研究电力线的高速带宽数据传输的成果。

电力线网络的结构在很多方面可以与有线网络类比，而且与本章中提到的Wi-Fi网络也有相似之处。

HomePlug 是第一个 PLC 的规范，它可以提供 1 ~ 5Mbit/s 的传输速率。另外，HomePlug 在网络连接设备方面采取了新技术，这些技术后面将详细研究。

HomePlug 规范仍在不断演进。随着版本的不断更新，数据传输速率不断提高，PLC 仍然受到媒介共享性质的制约。但是 HomePlug 在功能、服务质量和安全性等方面都有所改善。HomePlug 联盟在 PLC 标准化进程中占有重要的地位，不过我们从第 1 章可知，ETSI 和 IEEE 也已经开始了各自的标准化进程。

本章介绍了 PLC 网络的整个结构，并且对两个主要层（物理层和数据链路层）进行了详细叙述。

2.1　电力网络结构

PLC 技术通过电力线传输数据，因此电力线就成为了传输数据的媒介，与 OSI 模型中的物理层相对应。与其他物理层介质如 UTP（以太网线）、同轴电缆、光纤电缆等相比，传输数据并不是电力线最基本的功能。向公共电力网络的电气设备供电，是电力线的主要功能（在美国和日本传输电压为 110V/60Hz，在欧洲为 220V/50Hz），而利用电力线来传输数据则是电力线额外的功能。

根据电压不同，电力网络可按表 2.1 进行分类。

这种根据电压进行电力网络分类的方式，有利于相关单位根据各自职责进行分工。

表 2.1　电气电压值

当前的叫法	传统名称（仍在使用）	法国的通常电压值
HV	超高压	400000V、225000V
	高压	90000V、65000V
MV	中压	20000V
LV	低压	220V（单相）、380V（三相）

与国家电话公司的 PSTN（公用交换电话网）类似，配电网络中的发电厂是中心，配电网采用各种方式覆盖用户。这种网络是建立在星形结构的基础上，星形网

络的每个分支是连接用户和中心的电话线。

在 PSTN 中，中心局作为交换机，为在 20kHz ~ 1MHz 频段上用户调制解调器的 IP 流和在 300 ~ 3300kHz 频段上的传统电话通信提供服务。根据网络模型的解释，中心局既是以太网交换机，又是连接至 IP 骨干网的高速 IP 路由器（见图 2.1）。

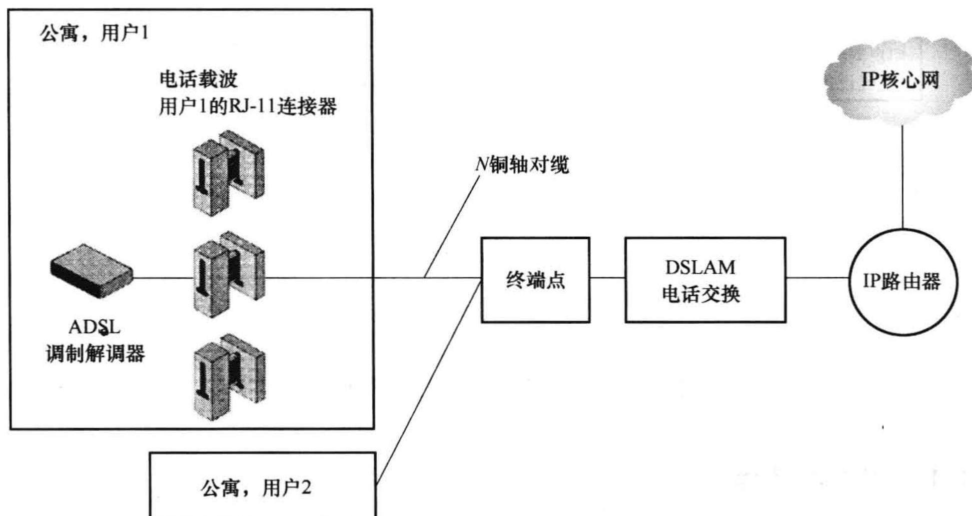


图 2.1 PSTN 网络结构的简单结构示意图

例如，在法国的电力配电网中，连接 MT 网和配电网的是 MV/LV 变压器，平均每个变压器服务 200 个法国电力公司的用户（见图 2.2）。MV/LV 变压器可以看作是 EGS 网络的以太网集线器，也可以看作是基于高速宽带 IP 传输链路的 IP 骨干网的网关。

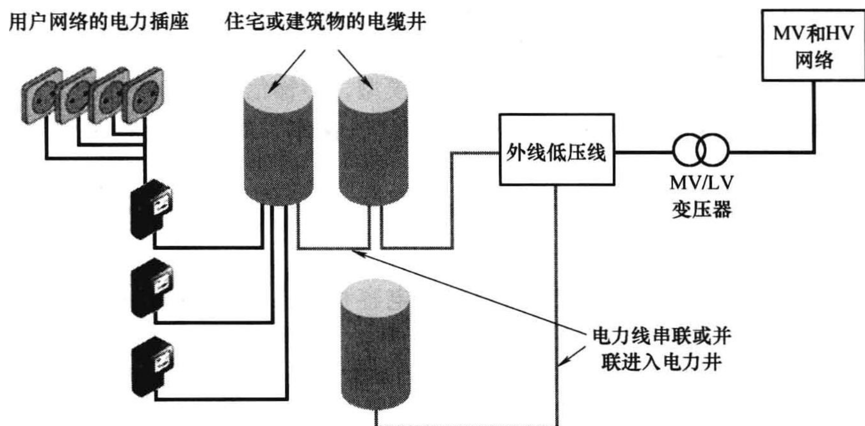


图 2.2 电力配电网络的简单结构示意图

根据不同的功能，电力网络每个部分的工作由不同组织承担，譬如说发电和输电。在 PLC 网络中，也有类似的情况。

图 2.3 反映的是国家电力网中各个组织履行的责任。

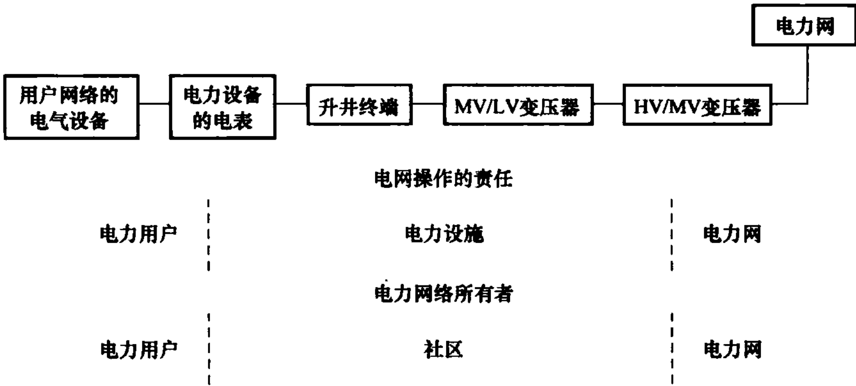


图 2.3 电力网络的操作责任分解图

2.1.1 电力线特点

PLC 技术的物理通道是电力线。电力线原本不是用来传输数据的，因此其物理特性参数的选取主要取决于电力传输，主要有电压和频率，例如 110V/60Hz。

这节介绍电力线的某些物理特性，这样便可以更好地理解电力线在数据传输方面的能力（包括优点和缺点）。

阻抗

电力线可以用阻抗 Z 来表征其特性（电力网络中各种组件的电阻、电感和电容的模值），它不是一个固定值。电气设备经常从电力网络上连接或断开，这改变了线路的阻抗，因此很难对通信媒介建立起模型，传输信道也是一样的。

与此同时，电气设备的阻抗是与工作模式、速率、时间、设计等情况相关的函数。

研究表明，典型的民用供电设备阻抗在 10Ω ~ 1kΩ 之间。

电容和电感

连接到电力网络中的各种设备都有一定电容和电感，其数值与电路中电流和频率（在 50Hz 或 60Hz 的线性变化）有关。

电路或电偶极子的电感（L）也被称为自感，其表示的是通过电路时电流的感应通量值。在具有非零磁导率（μ）的材料中，产生磁场强度（H）和磁感应强度（B）。

在有界表面的材料中，例如典型的电缆，电路中的电流所产生的磁场会引起感

应通量的变化，电感或许局限于电路，或者与其他电路相互作用。

电感可以用磁通量（Φ）和电流（I）的函数来表示，其公式为

$$L=\frac{\Phi}{I}$$

在正弦电压的情况下（家庭用电的情况下），用欧姆法则可以有效地表达这个关系式等式，这样一来，电感便是电压（U）、电流（I）、频率（f）的函数，即

$$L=\frac{U}{2\pi f I}(\text{单位是亨利,H})$$

电容（C）也称电路的容量，表达的是两个相邻的，带有相反电荷的导电表面体产生的电场中所蕴藏的能量值。

这个蕴藏的能量，也就是电容与形成电场的两个电偶极子中所带电量成正比。电量可以从电通量（Ψ）角度表示，并且与偶极子的两个表面之间电动势（V[⊖]）有关。

$$C=\frac{\Psi}{V}(\text{单位是库仑}^{⊜},\text{C})$$

在正弦电压的情况下（家庭用电的情况下），用欧姆法则可以有效地表达这个关系等式，这样一来，电容就是电压（U）、电流（I）、频率（f）的函数，即

$$C=\frac{I}{U2\pi f}\ (\text{单位是法拉，F})$$

电路的阻抗是由电阻（R）、电感（L）和电容（C）组成的，它们一起从电力角度完整地描述了阻抗特性。

这些特性作为网络中电流的函数，影响着整个网络的运行。从计算机科学方面看，这些特性形成了一个特别的物理层模型，旨在获取尽可能高的信道传输质量。

利用欧姆法则，阻抗可以用综合了电阻、电感、电容特性的复数来表示，j 表示复数的虚部。

$$Z=R+\text{j}(2\pi fL-\frac{1}{2\pi fC})\ (\text{取模值后，单位为欧姆}^{⊜}，\Omega)$$

当电流通过多个电路时，串联、并联的复杂网络阻抗形成它们的联合阻抗。每个部分随时都可能连接或断开。同样，各种阻抗会影响电流的产生，并影响到磁场和电场的产生。从信道传输的观点看，这些属性会有惊人的应用，我们在后续章节中将予以分析。

既然电感和电容特性的不断变化将直接影响到物理传输信道，那么 PLC 传输

⊖ 原书作者这里漏写了变量 V，现已补上。——译者注

⊜ 原书作者将电容单位描述为库仑，意为单位电压下的情况。实际上电容的国际单位是法拉。——译者注

⊜ 原书作者在表达阻抗时，可能因疏忽致公式有误，写成了 $Z=R+\text{j}2\pi fL+\frac{1}{2\pi fC}$。——译者注

技术就必须予以优化和加强。

电磁噪声和骚扰

由于电力线上或其周围连接有各种电气设备，传输信道就会存在有一定强度的噪声。

线路上或其周围的不同噪声类型如下：

1）电气设备关闭和开启的脉冲噪声；

2）宽带白噪声，即其功率谱密度在所有频率上相同；

3）在不同频率上的周期性噪声；

4）谐波噪声，其频率为网络中设备使用频率的线性倍数（如 50Hz 产生 300Hz、600Hz 等的谐波）。

总之，噪声用信噪比（SNR）来量化，通常用 dB 值度量。

除了电力线中的噪声，连接在电力网络，或者未连接但距离电力线很近的设备也会在传输信道上产生一定的骚扰电平。这种复杂技术问题被称为电磁兼容（EMC）问题。

从电磁兼容（EMC）观点看，每个电气设备都会产生电子干扰，它可能是传导式的（通过电力网网络传输）或者是辐射式的（在无线电环境中辐射）。

欧洲的 CENELEC 和国际 IEC 的许多工作组都建立了标准，明确包括电力线设备不同种类的电气设备骚扰权威的限值。同时，欧洲的 ETSI 和国际的 ITU 电信标准化组织也正在研究骚扰门限，优化传输信道，并且研究信号处理技术，使得 PLC 获得最好的性能。IEEE 也正致力于这类问题，以优化 OSI 模型中的物理层。

国际无线电干扰特别委员会（ISRIC）第三工作组在 150kHz 和 30MHz 频段上界定了 PLC 电气设备的骚扰允许限值。

PLC 收到的和引起的电磁兼容骚扰是另一个方面的研究课题。该课题的研究目标是对每一个（类）设备的发射电平制定标准，以便在此电平条件下得到高效的传输信道。

衰减

无线电信号通过电波传输时，其能量衰减是距离的函数；DSL 信号通过 PSTN 的同轴电缆时，其衰减也是距离的函数。与此类似，电信号能量同样也是传输距离的函数。

在使用 PLC 网络时必须考虑电力线的这些特性。正如在第 8 章（见表 8.10），为了使得 PLC 网络能提供更好的服务，我们将更加仔细地研究参数的选择。这些参数根据信号的距离函数以及衰减等情况有很大的差别。

电力网络的阻抗变化会在某些频率上导致多径效应，因其信号的开槽或者幅度激增。在家庭网络中，根据电力网络的内容和拓扑结构，电力线信号衰减在 20～60dB 范围内。

对于一个工作于20MHz以上频率的系统，其电能表和电路断路器的最小衰减为30dB。对于20MHz以下的系统，其平均衰减为50dB。而且，在某些频率下，好的PLC耦合器能将衰减减少10~15dB。

HomePlug1.0调制解调器的信号频率4~25MHz之间，其功率谱密度为-50dBm/Hz。我们可以在第8章的表8.10中看到这些值。

表2.2总结了重要电力线网络设备的衰减值。

表2.2　主要配电网络中电气设备的衰减

电器设备	衰　减	注　释
磁电式电能表	15dB	磁电式电能表使PLC信号衰减，但不截断它，导致私人网络的PLC信号可以向外传输
电子式电能表	15dB	与磁电式电能表相同
断路	5dB	如果连接两个PLC设备的线路经过太多的断路器，那么信号会大大衰减
插线板	10dB	插线板的结构质量对衰减影响很大，于是，我们应该避免将PLC器件接到插线板上
电子式电能表和断路器	20~30dB	在商业或家庭的非公共网络中，电能表和整合在一起的断路器不会给信号带来过大的衰减，因此也无法给PLC信号提供足够的保护
磁电式电能表和断路器	30dB 50dB	20MHz以上 20MHz以下

许多对家用电力配电网的研究表明，平均信号衰减为50dB/km。

相线之间的耦合

当电力线中存在高频变化的电信号时，它会在电力线附近产生磁场，这就称作耦合。

当感应耦合发生在同一电力网络的不同组件之间时，这种耦合称作串扰。如果是不同的电力网络，它们之间通过大地电流实现耦合。

频率响应

根据电力线的特性（材料、组成、年份等）不同，对高频信号的反应即信号的传播能力差别很大。

我们将在第8章（见表8.11）详细地说明使用PLC网络时这些特性的结果，以及当选择网络拓扑结构和电缆时怎样考虑。

接口灵敏度

电气设备中存在模拟接口，通过它们和电力线介质进行耦合（感性和容性）。PLC可以通过这些接口，在电力线上传输数字信号。

根据所使用的电子元器件，模拟接口的灵敏度特性使 PLC 信号传输中衰减不致过大。灵敏度可以用电力线和数字电路之间的阻抗来建模。

2.1.2 电力网络建模

对电力网络的建模可以让我们预测在数据传输中可能发生的现象（如骚扰、失去连接等），还可以提供一份最能支持网络工程应用的描绘图。

无论电力网络用在公众范围（公共配电网络）、私人网络还是商用网络，对其建模是一个需要考虑许多参数的比较困难的技术课题（如拓扑结构、电力线性质、骚扰、连接到网路中的设备、时间等）。

鉴于对电力网络而言，还没有完备的建模工具，因此 PLC 网络工程的仿真建模还受限于对 PLC 信号物理层的建模。

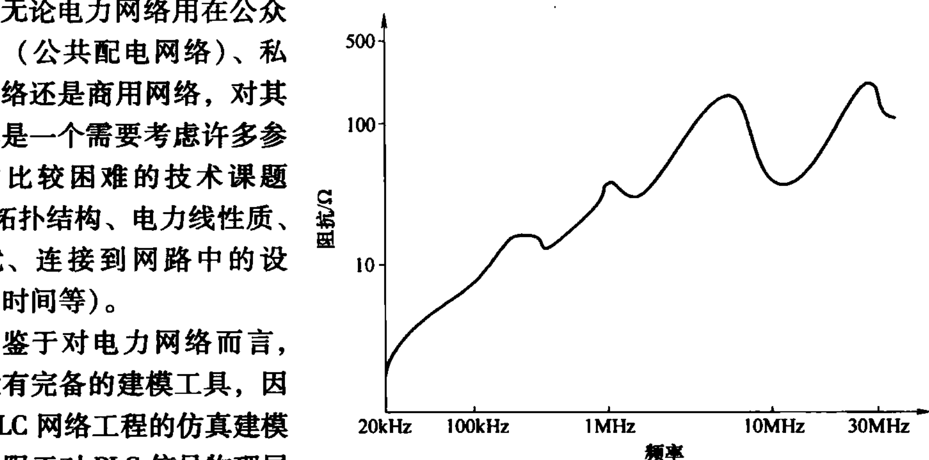


图 2.4 电力线作为频率函数的平均阻抗

通过对电力网络的测量，我们可以获得高频时 PLC 设备的平均阻抗。

图 2.4 反映的是以频率为函数的阻抗曲线（单位为 Ω 且为绝对值）。对 PLC 而言，这种阻抗在 5 ~ 150Ω 之间变化。

经 Nicholson 和 Malak 研究，我们可以用以下公式来表示电力线的平均阻抗：

$$Z_c = \sqrt{L/C}$$

式中，L 为电力线的线性电感，μH/m；C 为电力线的线性电容，μF/m。

Downey 和 Sutterlin 的研究工作表明，我们可以将电路等效为一路电力线。这路电力线由阻抗、电容、电感组成，其系统组成如图 2.5 所示。

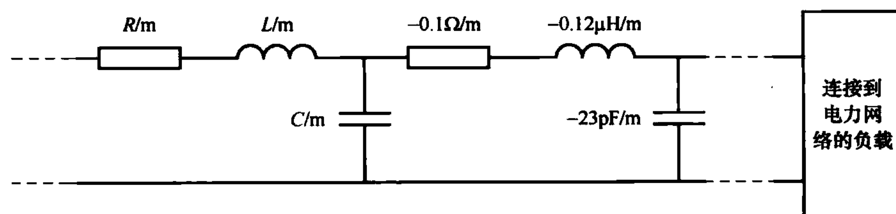


图 2.5 作为 Downey 和 Sutterlin 模型的电力线主要电路

我们可以用下面的等式描述电力线阻抗：

$$Z = R(f) + sL(\text{单位是}\ \Omega)$$

式中，R 是电缆的阻抗，是电缆中传输信号频率的函数；s 是电缆的直径；L 是电力线的电感。

阻抗与连接在电力线中的负载有关，连接于电力网络中的电器设备（吹风机、钨丝灯等）每个都具有自己的特性阻抗。

利用这些建模元素，我们可以计算电力网络的特征值，这种特征值会影响 PLC 中信号的传输。

网络中电气设备的建模

对电力网络的建模比较困难。同样，对连接在网络中的电气设备的建模也很困难。由于各种设备以不可预见的方式与网络连接或断开，导致网络负载的不连续变化。

设备的特性也会根据年限、使用时间、使用频率等的不同而变化，因此这种建模会非常不精确。

随着电磁兼容技术的发展，我们将实现对整个电力网络的建模，并且能够根据网络的基于线路拓扑结构的函数进行建模。这样，将会出现一些有利于理解工程和电力网络中电力线信号的特性模拟工具。

此外，CENELEC（欧洲电工技术标准化委员会）正在开发一种能够对家庭电网进行建模的系统。

2.2 共享介质结构

第 10～12 章主要叙述家庭、商用、社区的 PLC 网络的工程安装。我们可以看到，电力网拓扑被看成是承载多路 PLC 信号和传输局域网的终端间交换数据的共享媒介。

在那些章节中，我们将区分“公共”网络和“私人”网路，“公共”网络是提供电力给个人、商用以及社区的网络。“私人”网络由一栋建筑的配电网组成，从电能表到插座。我们可以看到，对于这两种网络而言，共享媒介的概念是相同的。

2.2.1 公共网络

公共电力网络是在邻里、小镇、社区里能够为房子、公寓、建筑和商业服务的配电网络。这种公共网络在某种程度上对任何人都是公用的，任何人都有可能成为用户并且获得当地电力网络的授权。

图 2.6 反映的是一个公共电力网络中有 6 个电能表，每个电能表背后都有 PLC

设备连接在家用的私人网络上。根据公共电力网络的拓扑结构（如星形、环形等）和分支，电能表之间的电力线可以共享。

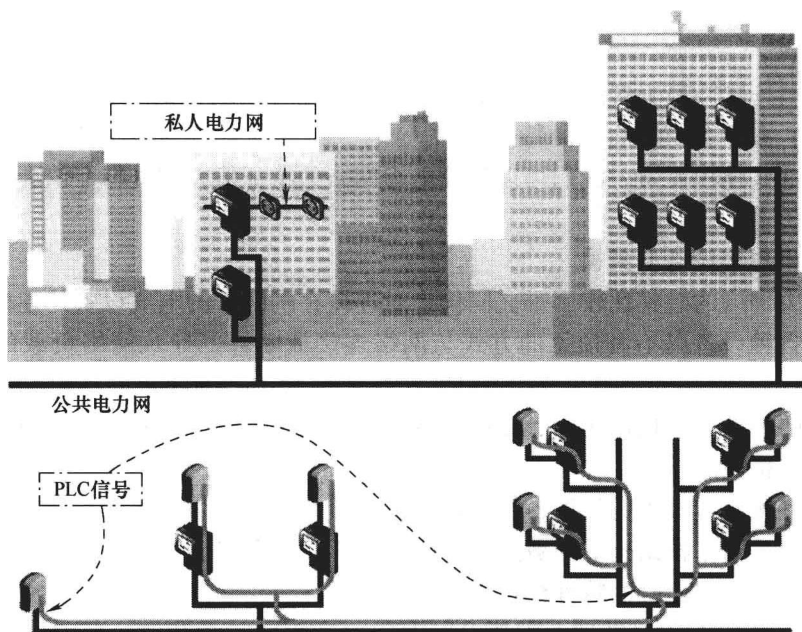


图 2.6　看作共享媒介的公共电力网络

在这个图中，两个电力支路在几个电能表和 PLC 设备那里终止。PLC 信号沿着这些包括电能表和电路断路器的支路，在不同网络的设备上传播。与之相关的问题是信号在电力线间的衰减。因此，我们可以这样来看，即电力网络是一条数据总线，线上的 PLC 设备既连接着公用区域，又连接着私有区域。

2.2.2　私人网络

私人网络位于公共电力网络的电表后面，由其所服务的公寓、房间、办公室、工厂等区域来管理。

这种网络的拓扑结构，不像公共电力网络，其不遵循清晰的工程规则，可能存在特殊的情况（如网络的附加部分、电路断路器面板或串行拓扑结构等）。然而，网络所有分支源于电能表和主电路断路器，PLC 信号都通过电路断路器面板传输。

图 2.7 反映的是带有电路断路器的 3 个分支的电力网络的简化模型。在示意图的右边，PLC 信号在连接 PLC 设备的各插座之间进行传播。这个例子反映了私人电力网络可以被看作是一个等效于数据总线的共享媒介。

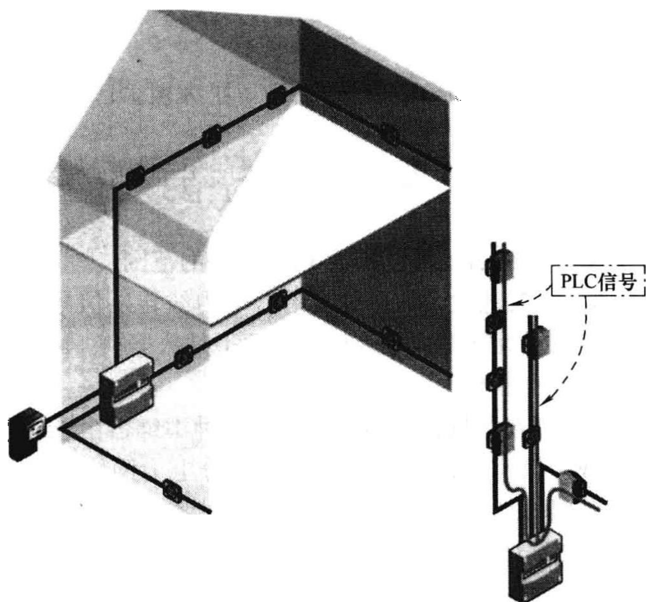


图 2.7　看作共享媒介的私人网络

2.2.3　与网络集线器类比

前面的有关公共和私人网络的两个例子说明，任何类型的电力网络都可以看作是具有巨大容量的数据总线，PLC 设备连接其上。、

从通信设备角度看，拿网络集线器来类比是再恰当不过的，因为 PLC 连接到电力网络上，并代表着不同的以太网端口。图 2.8 反映了这种情况。

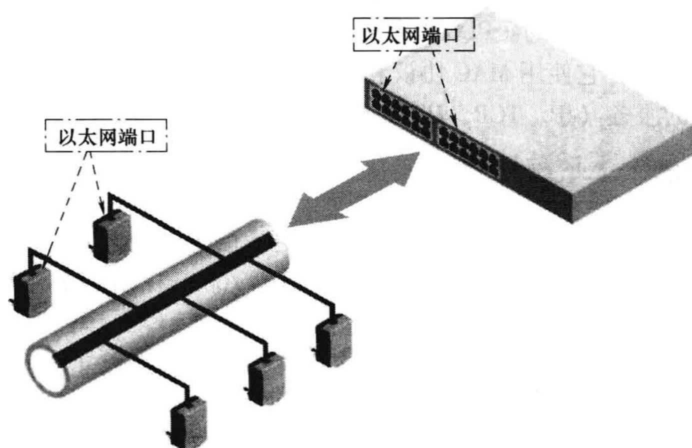


图 2.8　PLC 网络和转发器间的模拟

2.2.4 PLC 中继器的概念

在第7章将可以看到，对于PLC设备，为了扩大覆盖区域和连接更多的设备，对信号进行中继非常必要。

当在电力线中PLC信号变得太弱，不能给网络中的PLC设备使用时，中继器就需要对信号进行放大再生。

这里有两种类型的中继器，可以扩大PLC网络的范围。

1）物理中继器，真实地放大信号并且沿着电力线转发信号。这种类型之所以被称为物理的，是因为它对物理信号进行操作而不是数据帧。因此，这种转发器不会降低整个电力通信网的带宽。

2）逻辑PLC中继器在数据帧上转发数据。这种中继器由连接在以太网接口上的两种PLC设备组成：第一种设备用于连接一部分电力网络；第二种设备连接于因过多地衰减PLC信号难以到达的那部分网络。这种中继器降低了整个PLC网络的带宽，因为，它在相同的物理电力网络下构建了两种不同的逻辑网络。

2.3 分层结构

OSI（开放系统互连）分层模型描述了任何数据网络的共同基础。这种模型由七层组成，每层都有一个独立的协议，每层协议在为上层提供某种服务的同时需要其下一层的某种服务支撑。

在这种模型中，PLC网络与第一层（物理层）和第二层（数据链路层）有关，数据链路层向上层提供以太网链接服务。

图2.9反映了PLC技术在OSI模型中的位置，第一层（物理层）是通过传输PLC信号的电力线来实现的。PLC设备提供具有与第二层相关的以太网链接服务终端（典型的如PC），它使用MAC协议和RJ-45连接器。这种终端用PLC网络服务接入到更高层的服务（IP、TCP、HTTP等）。

2.3.1 物理层

PLC技术的物理层是通过电力线来实现，更通俗的说是电力网络。为了在媒介中传输PLC信号，此电路的线路频率（例如110V/60Hz）由一个在某个中心频率（载波频率）f附近的小幅度信号调制后提供。

因此，物理层包括这种在电力线中以某个频率传输的低幅度调制信号，其频率是由PLC技术和恰当的规则决定。我们将在第3章仔细讨论调制技术。

图2.10反映了功率信号和PLC的总和，此信号加载在电力线上，形成了PLC网络的物理层。

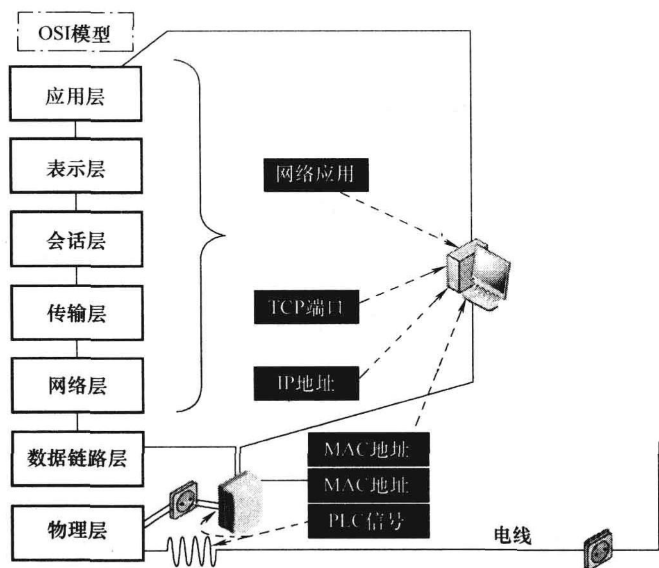


图2.9　OSI模型中PLC的位置

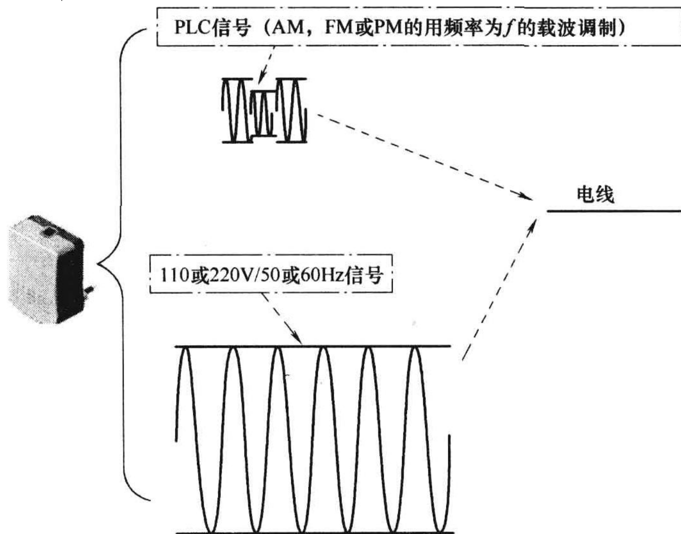


图2.10　调制的PLC信号和电力线信号的叠加

2.3.2　频带

PLC信号是在某个载波上对幅度、频率、相位进行调制。国家级和国际级的标准化组织在0～10GHz建立了每个频带的使用规则。

两个频带分配给 PLC 技术。

1）3 ~ 148kHz 作为低传输速率的 PLC。

2）2 ~ 20MHz 作为高传输速率的 PLC。

图 2.11 所示为 PLC 与其他相关网络技术在频带上的位置关系。

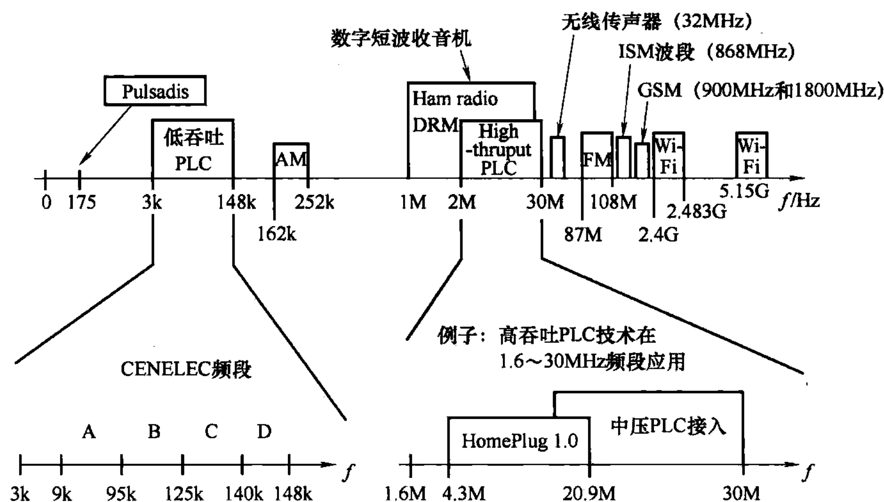


图 2.11 分配给 PLC 网络的频带

第3章　功　　能

本章将介绍PLC网络的功能。由于在这些网络中所使用的技术易于集成到简单的芯片中，所以网络组件的制造成本相当低。这些网络组件与引入的PLC接口密切相关，最终目的就是为了提高设备的吞吐量。

PLC利用了固定网络中许多成熟的技术，特别是ADSL、Wi-Fi、以太网技术等。PLC电气组件采取了必要的技术使得PLC链路稳定可靠，克服了这类网络结构的主要薄弱点。

PLC主要功能如下：

1）网络模式：用于各种PLC设备之间的网络管理和通信。

2）PLC帧管理模式：用于解决大量数据流传输问题，特别是数据的分包和重组。

3）媒介接入技术：包括网络设备的同步和优先权的管理。

4）服务质量：在PLC环境下提供语音、视频数据的传输。

3.1　网络模式功能

PLC网络一个最主要的功能就是网络模式，用来管理同一网络中的所有PLC设备。

根据定义，网络是由几个互相交换数据的设备所组成的。因此，为了实现设备之间交换数据的组织性、最优性，有必要建立一个交换管理系统。

下面是3种网络组织模式。每种PLC技术使用其中的一种模式。

1. 主-从模式（master-slave mode）

类似于IP网络中的客户端—服务器的IP网络模式。在IP网络中存在一个主设备，管理网络中PLC设备之间的数据交换，从设备根据主设备的管理要求相互进行数据交换。

2. 对等模式（又称点到点模式，peer to peer mode）

类似于IP网络中的对等模式。在这种模式中，网络中所有的PLC设备都扮演着同样的角色，地位是相同的。这些设备不需要在主设备的监视下进行数据交换。

3. 集中模式（又称中心模式，centralization mode）

这是上述两种方式的折中。网络中存在一个中心设备来负责管理PLC设备之间的交换。其他设备不用经过中心设备也可以与另外的设备进行数据交换。

表3.1归纳了这3种模式的优缺点。

表3.1　主-从模式、对等模式和集中模式的优缺点

模　式	优　点	缺　点
主-从模式	集中管理 PLC网络的网关作用 QoS等级管理（TDMA） 每个设备的角色管理 PLC和IP网络分层 网络监管更容易	需要冗余 安全性的弱点 可能造成带宽拥塞 配置更复杂
对等模式	带宽分布 物理层PLC路由列表分布 易于部署	无网络分层 PLC网关无清晰定义
集中模式	集中式管理 只有管理业务流通过协调中心	集中式的缺点 需协调管理TDMA帧

3.1.1　主-从模式

电力网络由电能表、断路器和总线组成。电能表位于电力网络的顶端，可视作电力网络的主设备；断路器与总线可视作从设备。PLC网络的主-从模式根据电力网络的这种逻辑结构，在这种物理媒介上，将主设备放置在网络的顶端，从设备放置在网络的各个枝干上。

在公共MV或者LV电力网络的主-从模式的PLC网络中，主设备的功能可能有：

1）各种从设备的安全连接管理。由于有专门的信道与用作公共媒介的电力线相连接，因此每个设备都归属于一个私人逻辑网络。PLC数据帧可以自由地在电力网络中的各个枝干上进行传输。

2）通过对各种物理层的分析（如每个频率子带上的信噪比、计算每赫兹上的传输数据量等），实现主-从设备之间PLC物理链路的QoS（服务质量）管理。QoS管理是通过使用一张质量表单，对位于PLC主设备层面的各种连接进行衡量而实现的。

3）通过位于物理层或者可能位于逻辑层的集中管理的加密密钥，使得建立VLAN或者是从设备之间的链路成为可能。

4）监管设备，根据更加复杂的IP网络结构，将IP网络管理工具（SNMP堆栈类型）向上集成到PLC网络中。

5）主设备之间冗余度的管理。

主设备整合整个PLC网络的管理智能，通过嵌入式或远程接口接入标准协议，

如 HTTP、IP，提供优化的结构管理，能够根据电力网络的起伏波动，不停地更新 SNMP 堆栈。

在类似家用的低压电力网络的 PLC 网络（如公寓、住宅、医院、旅馆、学校等）中，各种主设备（即在电力网络中可能存在的用来构成特定的网络或者用来中继 PLC 信号的几种设备）可能的功能如下：

1）管理主-从设备之间以及从设备之间的 PLC 连接质量。

2）通过使用有用的网络参数（与 TCP 层有关），例如起伏或者延时等，实现服务质量的管理。

3）在每一个逻辑网络中使用加密密钥实现安全连接管理，确保每个 PLC 从设备（如旅馆、学校公寓大厅的架构）的逻辑隔离。这项功能主要用于检测新加入到网络的设备或者是已经加入的设备。

4）主设备之间冗余度的管理，目的是确保在吞吐量高达 200Mbit/s 时整个 PLC 架构的正常运行，以及将来在物理层实现更高的吞吐量。

表 3.2 总结了主设备可能的主要功能以及相应的技术解决方案。

表 3.2 主设备和对应技术结论预计的性能

性 能	技术解决方案
帧冲突	CSMA/CA
时分复用	TDMA
物理层链路状态列表	载波列表
50Hz 网络帧同步	过零
每个频率子带的信噪比	侦听噪声电平
MAC 层监督	帧和 FEC
监督帧	指示标志区域化和指示模式

3.1.2 对等模式

通信网络理论主要是基于网络设备分级的原理。随着 Ad Hoc 类型架构的出现，无论是在无线局域网还是在对等网络中（在因特网上进行文件交换），这种理论均遭到质疑。与分级结构的网络或者是主-从模式的网络相比，非集中式的网络有许多优点。

图 3.1 描述了对等模式的 PLC 架构，所有的 PLC 设备都扮演着相同的角色，而且为了保持网络的协调，PLC 设备不停地进行参数的交换。在 HomePlug1.0 中，设备也在局部进行着数据的交换和信息的更新。

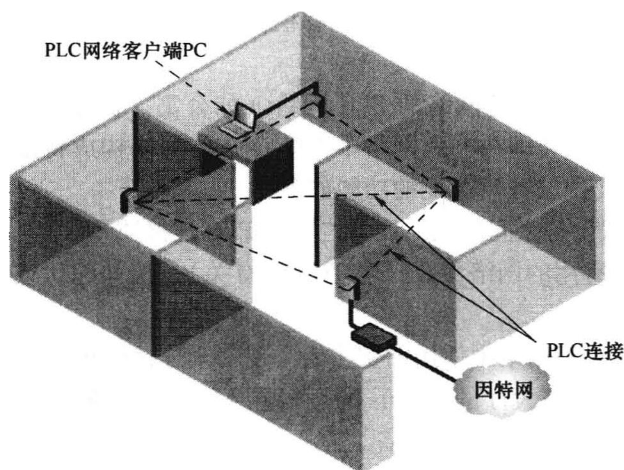


图 3.1 对等模式的 PLC 网络架构

PLC 设备的主要参数如下：

1）设备和其他设备之间的 PLC 链路的质量。对这一质量的衡量是在物理层进行的，并且该衡量方式与对无线电设备的无线链路质量进行衡量从而评价 OSI 高层的可用服务十分相似。这种质量的衡量是通过不断更新一个列表来实现的，这个列表又称作“载波列表”（tone map table）。

2）用于连接 PLC 网络和与其他设备进行交换的加密密钥的选择（EKS）。在 HomePlug1.0 中有两种 EKS：DEK（默认加密密钥）和 NEK（网络加密密钥）。我们将在第 4 章介绍它们的特性，包括安全性。在第 9 章将要介绍它们的配置。在同一电力网络中，这些密钥被用于建立几个对等模式的 PLC 网络，但是这些网络并不相互传输数据信息。由于建立的对等模式的 PLC 网络都使用 2～30MHz 的全部频谱，因此各个网络的吞吐量可能会降低。

3）基于 PLC 链路的质量，最适合的调制方式和 FEC（前向纠错）类型。在 HomePlug1.0 中，有 4 种可使用的调制方式：DQPSK 3/4（差分正交相移键控）、DQPSK 1/2、DBPSK 1/2（差分二进制相移键控）和 ROBO（增强型 OFDM），分别用于 4 种不同速率传输。

4）每个网络 PLC 设备的优先权。对于每一个 PLC 设备而言，根据它的配置，这项参数可以在以太网帧的 VLAN 区域获得。该参数被用于建立设备的网络等级，通过这个参数，可以指定那些充当相对与其他网络连接的网关角色的设备以及那些在架构中充当标杆角色的设备。

图 3.2 是对等模式的 PLC 网络架构示意图。为了保持网络的同构性和维持更好的以太网帧和带宽路由分配，上述 4 种参数均被网络中的设备进行不停的交换。

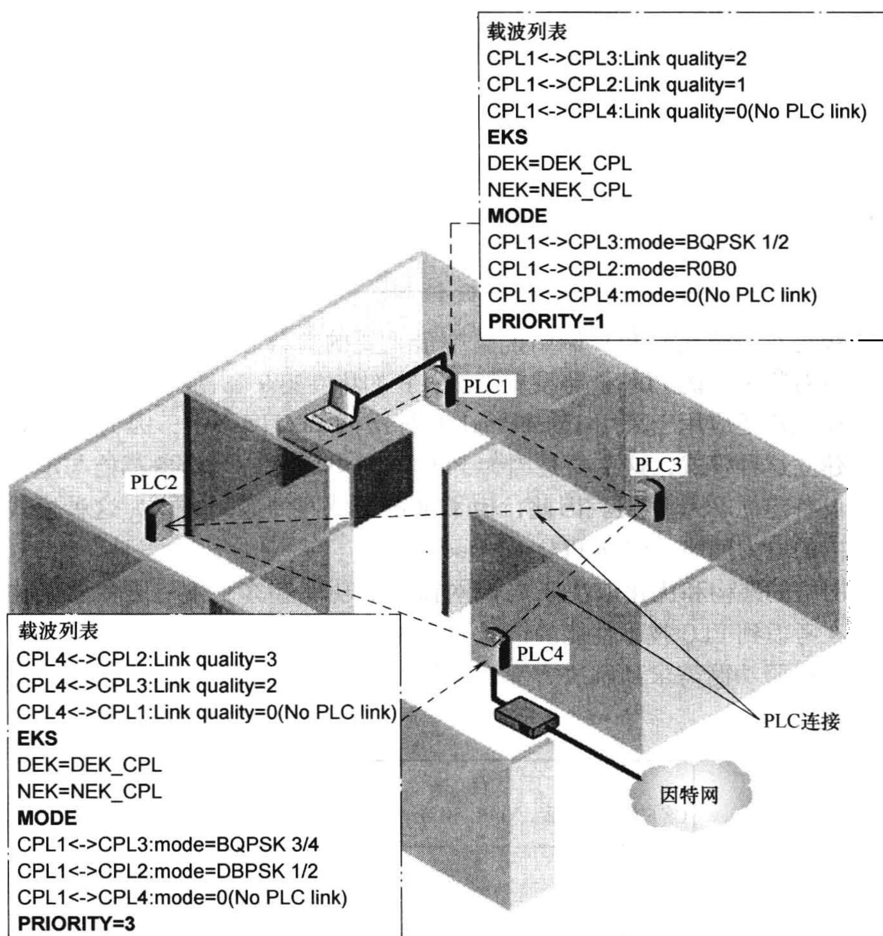


图3.2 对等模式的PLC网络设备间的参数交换

基于优先级的HomePlug1.0 PLC网络分级

在IEEE802.3以太网帧结构中，VLAN域可能在IEEE 802.1q标准中加以叙述。在对等模式的PLC网络的架构中，该域则用于创建同一网络中PLC设备之间的等级。该域按3bit进行编码，因此有8个值。

表3.3是根据VLAN域的值列出的4种可用的PLC优先级。

用作与其他网络连接的PLC网关设备或者连接到服务器的PLC设备应当定义为较高的优先级，这样做的好处是能够更多地接收到来自其他网络中由PLC设备承载的作为客户端与上述服务器上相连接的PC设备发出的数据。一些连接到IP网络电话的PLC设备其优先等级定义为4，这样就能够为实时语音通信提供最好的传输。

表 3.3 VLAN 域的 PLC 优先级

优　先　级	VLAN 域的值	应 用 分 级
优先级 3	6，7	VoIP（传输时延小于 10ms）
优先级 2	4，5	基于 IP 的视频（传输时延小于 100ms）
优先级 1	2，3	未加工数据的传输和控制数据
优先级 0	0，1	有限的数据通信

优先级是对等模式的 PLC 网络配置中最主要的参数之一，尽管它只是一个逻辑参数，且对物理层的 PLC 链路没有影响。我们将在第 9 章再次讨论这个参数。

对等模式广泛应用于采用 HomePlug1.0 标准的 PLC 网络中，因为 PLC 网络能够快速地建立这种模式，这主要是因为 PLC 网络中的每一个设备都能与电力网络插座上的设备建立 PLC 链路。因此，为了满足局域网的应用需求，这种模式用于在建筑物内的电力网络上建立 PLC Ad Hoc 网络。

PLC 网络的架构和优化取决于局域网预期的功能和客户端—服务器架构的需求，从而在考虑到 PLC 技术性能的情况下实现一个现实的架构。

图 3.3 按照功能需求到解决方案的顺序，介绍了建立对等模式 PLC 网络的各个步骤。

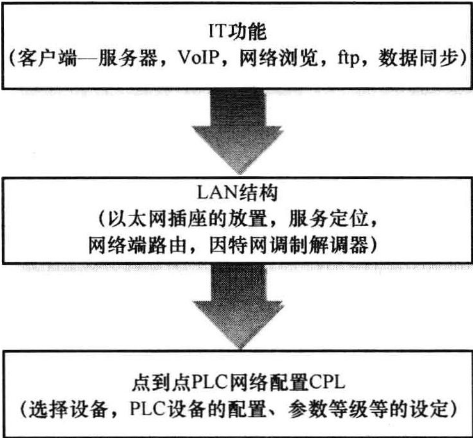


图 3.3 对等模式的 PLC 网络的建立

3.1.3 集中模式

实际上，HomePlug AV PLC 技术的架构既不是对等模式也不是主-从模式。它涉及两种设备类型：具有相同等级的设备和中心的设备，如图 3.4 所示。

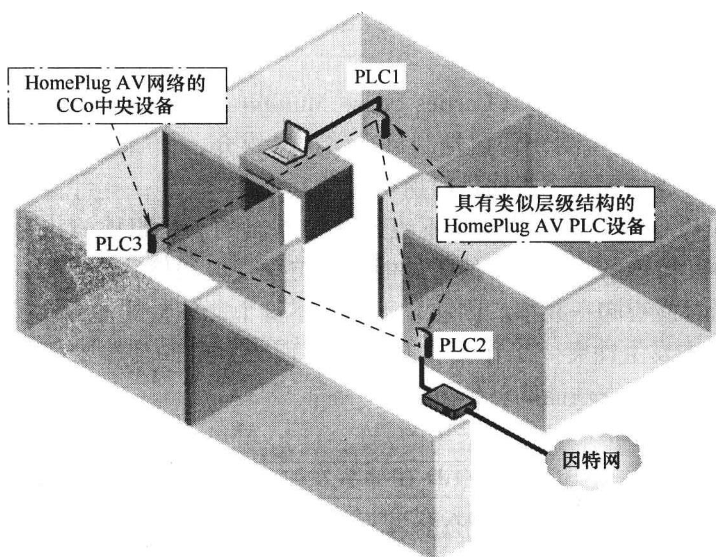


图 3.4 集中模式的 PLC 网络结构

CCo（中心）设备为各个需要进行通信的 PLC 设备进行媒介接入分配的管理。

在 PLC1 和 PLC2 设备之间进行数据通信，需要遵循以下步骤：

1）PLC1 和 PLC2 进行传输通道估计（调制、纠错等）。

2）PLC1 和 PLC2 通知 CCo（PLC3）要进行数据交换。

3）CCo（PLC3）分配给它们一个时隙，在这段时间内它们能够接入传输媒介。

4）PLC1 和 PLC2 不需要经过 CCo，直接传输数据信息。

若 CCo 中心设备负责管理媒介接入看作是主-从模式，那么数据能够在设备之间直接进行传输就好比是对等模式一样。

3.2 传输通道功能

在 PLC 中，传输通道是电力网络。因为传输通道最初并不是为网络应用而设计的，所以为了保证数据链路的正常运行，不得不添加网络功能模块。其中媒介接入、帧同步和电力线上的频率管理程序对于 PLC 技术而言是特定的。

3.2.1 使用 CSMA/CA 技术接入媒介

CSMA/CA（Carries Sense Multiple Access/Collision Avoidance，载波侦听多路接入/避免冲突）是一种侦听载波的随机接入技术，在发送数据之前侦听传输媒介。

CSMA 能够防止多个传输任务在同一时间、同一媒介中进行，从而减少冲突，但不能完全避免。

在以太网中，CSMA/CD（Carries Sense Multiple Access/Collision Detection，载波侦听多路接入/冲突检测）协议控制每个站接入媒介，侦听和处理当两个或多个工作站需要同时通过网络进行通信时所引起的冲突。

不过，在 PLC 网络中，冲突是不容易被检测出的。要想检测出冲突，一个工作站必须具备在传输的同时进行侦听的能力。与无线电通信系统类似，PLC 系统不能在传输的同时侦听同一频率。因此，工作站本身不能侦听到冲突。有鉴于此，即便 PLC 在传输中发生冲突，工作站自身也不能侦听自身的传输，而是继续传输完整的帧，这会造成网络性能的整体下降。

考虑到这些具体特点，PLC 采用的是修订的 CSMA/CD 协议，即 CSMA/CA 协议。CSMA/CA 协议并不像 CSMA/CD 在冲突发生后才去反应。因此，CSMA/CA 力图通过避免冲突的发生和获知接入媒介时所发生的冲突的最大概率来减少冲突数目。

为了避免冲突，CSMA/CA 采用各种技术，如 PLC 引进的媒介侦听技术；媒介多重接入管理的退避算法；一种通过确认媒介是否空闲从而解决冲突次数的可供选择保留机制；以及主动确认帧（ACQ）。

与 Wi-Fi 中使用的 CSMA/CA 相比，在 PLC 中使用的 CSMA/CA 有所不同。在 HomePlug 标准中使用了一个数值来说明，当与相同优先级的工作站对比之后，一个工作站不能发射（传输）数据的时长。这个时长的值叫做 DC（延时计数器），当工作站不发送数据时，该值增加，这就为有相同优先权的工作站使用网络提供了可能。

图 3.5 表示整个的 CSMA/CA 算法流程。

侦听媒介

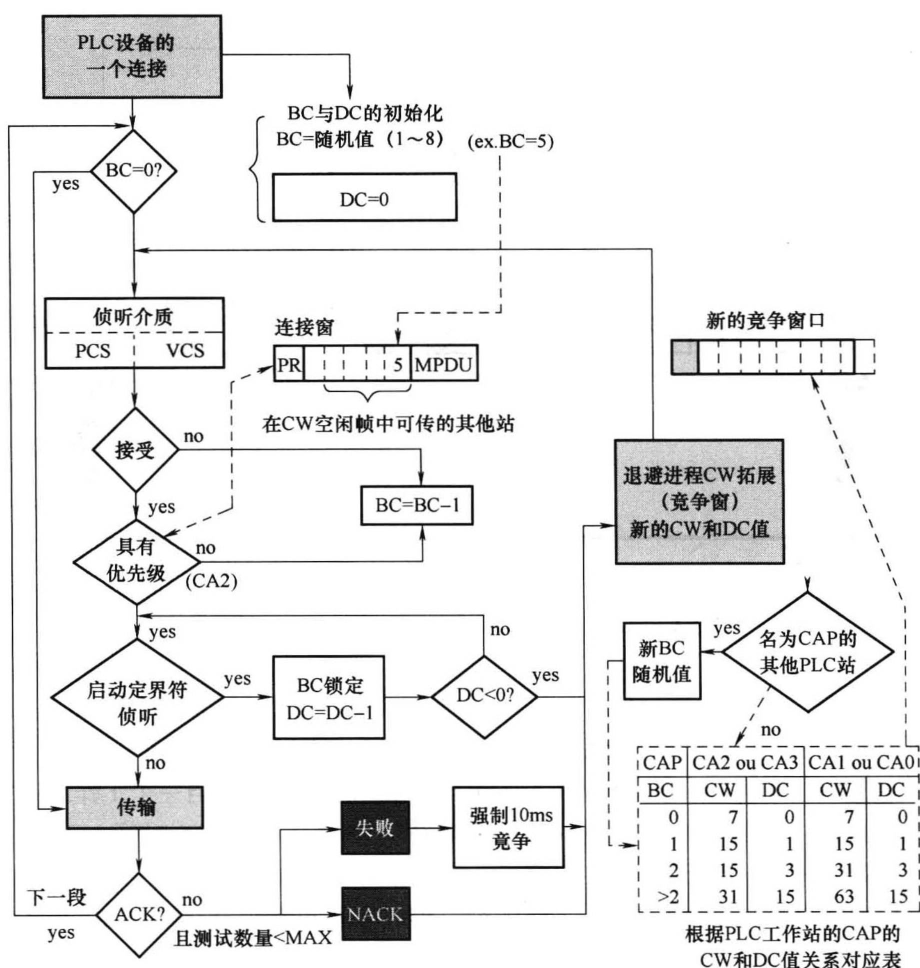
在 PLC 中，媒介分别在物理层和 MAC 层被侦听，在物理层使用 PCS（Physical Carrier Sense，物理层载波侦听），在 MAC 层使用 VCS（Virtual Carrier Sense，虚拟载波侦听）。

通过侦听其他 PLC 工作站，分析接收到的数据帧，或者是通过借助于来自各工作站信号的相关功率侦听媒介活动，PCS 能够获知媒介的状态。PCS 技术主要是依靠侦听特定的接收帧（received frames）、前导帧（preamble frames）和优先权帧（priority frames）。

实际上，VCS 并不是真正地侦听媒介是否空闲，而是通过使用 PCS 来保留（或预留）媒介。

VCS 中使用两种机制：

1）在帧头的区域检测；



CAP	CA2 ou CA3		CA1 ou CA0	
BC	CW	DC	CW	DC
0	7	0	7	0
1	15	1	15	1
2	15	3	31	3
>2	31	15	63	15

图 3.5 HomePlug 1.0 CSMA/CA 操作

2）等待由帧控制区域提供的反应信息。

图 3.6 阐述了在数据传输之前这两种侦听技术。

接入媒介

IFS（Interframe Spacing，帧间间隔）机制用于控制媒介接入。这个间隔与两帧传输的时间间隔相一致。事实上，IFS 是媒介传输的空闲周期，用于管理工作站的媒介接入和建立传输的优先级系统。

各种类型的网络的 IFS 值取决于物理层。HomePlug1.0 标准定义了 3 种类型的 IFS：

1）CIFS（Contention Distributed Interframe Spacing，竞争分布帧间间隔）。那些期望接入媒介的工作站在媒介空闲时使用这个 CIFS 直到其他传输开始，这个过程

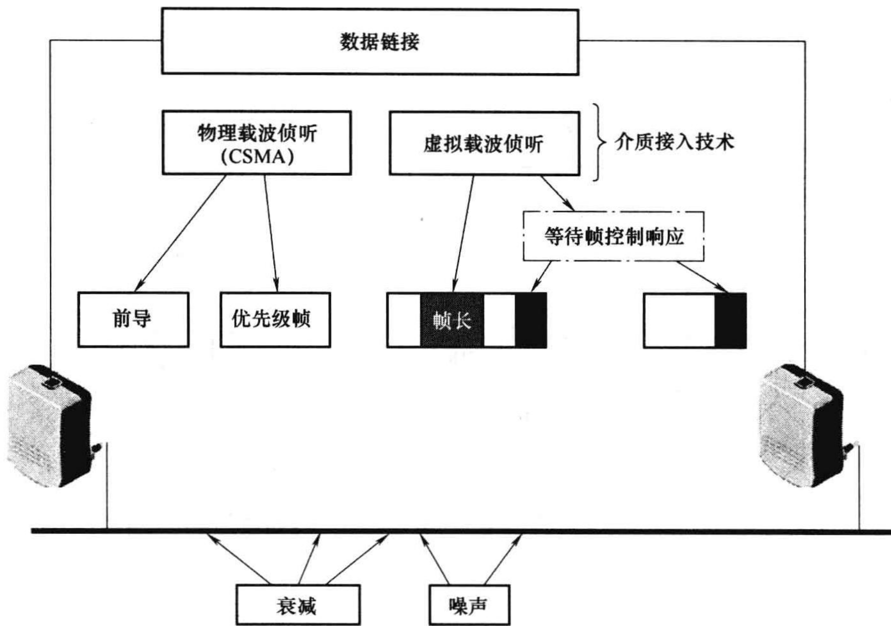


图 3.6 在 HomePlug 1.0 中侦听媒介

为 35.84μs。在 CIFS 之后，就是每个工作站的优先级解决方案阶段。

2）RIFS（Response InterFrame Spacing，响应帧间间隔）。当一个工作站等待来自终端的响应时，终端在传输响应之前先等待一个 26μs 的 RIFS 时间。RIFS 也被工作站用于将发送模式转换为接收模式。

3）EIFS（Extended Interframe Spacing，扩展帧间间隔）。EIFS 与工作站传输需要的最大时长一致。它等于非 ROBO 模式下传输数据帧的时间加上若干定界符号时长（即为 CIFS、RIFS 和帧间隔结束符（End of Frame Gap，EFG））的总和，计 1695μs。EIFS 被用来确定发生冲突后媒介被占用的时间。在前向纠错控制中，EIFS 被用于检查接收数据是否存在错误。当使用 VCS 方式侦听媒介时，对帧的长度进行的测量并不是采用全力（fully robust）方式的。

表 3.4 归纳了 HomePlug1.0 和 HomePlug AV 中的 IFS 值和时隙值。

表 3.4 基于物理层的 IFS 值和时隙值

	HomePlug1.0	HomePlug AV
时隙	35.84μs	35.84μs
CIFS	35.84μs	100μs
RIFS	26μs	30～160μs，140μs（默认）
EIFS	1695μs	2920μs

（续）

	HomePlug1.0	HomePlug AV
AIFS	—	30μs
B2BIFS	—	85μs
BIFS	—	20μs
CIFS AV	—	100μs
RGIFS	—	80μs

HomePlug 标准的 AV 版本与 1.0 版本相比，包含了许多补充的 IFS。

1）AIFS（Allocation Interframe Spacing，分配帧间间隔）。用 AIFS 将 TDMA 和 CSMA/CA 分配区域从在 HomePlug AV 标准中的预留业务中分离出来。

2）B2BIFS（Beacon to Beacon Interframe Spacing，信标-信标帧间间隔）。将特定的 TDMA 分配区域的各种信标帧从 HomePlug AV 信标帧中分离出来。

3）BIFS（Burst Interframe Spacing，突发帧间间隔）。在突发类型网络模式中接入 CSMA/CA 媒介时，BIFS 用于将各种 MPDU 帧进行分离。

4）CIFS AV（Contention Distributed Interframe Spacing Version AV）。想要接入媒介的工作站利用 CIFS AV，将来自于源工作站的传输帧和来自于终端工作站的响应帧进行分离。

5）RGIFS（Reverse Grant Interframe Spacing，预留开放帧间间隔）。具体到 HomePlug AV 标准，RGIFS 被用于在预留开放网络模式中进行帧分离。

退避算法

根据前面的分析，PLC 使用 CSMA/CA 方法来控制传输通道的接入。

由于电力媒介中的衰减和噪声，且冲突无法被检测出来，所以只有当媒介能够被用于传输的时候，PLC 工作站才能开始传输。直到 IFS 空闲一段随机的时长后，工作站才能传输数据，将这个时间段称为退避时间。因为在此期间并不能保证不发生冲突，所以源工作站必须要等待终端工作站发送的 ACK 信号。如果接收到的数据是正确的，那么终端就发送一个好的接收响应。ACK 响应在下一个可用的 IFS 期间进行传输。

在 PLC 中，将时间切割成一片一片的，或者称之为时隙。为了保证在这些时隙内能够以相等的概率接入媒介，就需要一个计时器统一管理这些时隙，且这个计时器必须适用于各种工作站的传输和重传。

退避算法定义了一个 CW（Contention Window，竞争窗）或者称作退避窗。这个参数与挑选出的可用来计算退避时间计时器的时隙数量是一致的。

HomePlug 标准中预定义了 CW_{min} 和 CW_{max} 数值。当媒介处于工作状态或者是源工作站没有接收到终端的 ACK 信号时，退避进程就使用 BC（退避计数器）来计算

时隙的数量（也就是前面提及的挑选出的可用来计算退避时间计时器的时隙数量）。一旦工作站想要传输信息，就采用先前定义的 PCS 方法侦听媒介。

如果媒介是空闲的，那么工作站将延迟一个 IFS 传送数据。当 IFS 时间结束时，媒介仍旧空闲，工作站将直接传输它的帧而不需要再使用退避算法。若媒介被其他的工作站使用，那么该工作站就要等待媒介空闲，换句话说就是要延迟它的传输。

为了再次接入媒介，工作站需要使用退避算法。如果有几个站同时在等待传输，那么它们都要使用该算法。各个站可以忽略连接到网络的其他工作站。如果不使用这种机制，而是各个站都潜在地计算一个不同的退避时间计时器来延迟它的传输，那么一旦媒介被释放，这些工作站就有可能彼此发生冲突。

工作站根据以下公式来计算自己的计时器，用 T_{BACKOFF}来表示，即

$$T_{\mathrm{BACKOFF}} = \mathrm{Random}(0, \mathrm{CW}) \times \text{时隙}$$

其中，Random（0，CW）是在［0，CW－1］服从归一化伪随机分布的变量。因此，T_{BACKOFF}是对应于时隙的数目。对于每个工作站来说，这个参数能够随即得到各种计时器值。

图 3.7 给出了在不同重传输数目的条件下，竞争窗口（CW）和传输失败计数器（DC）的取值。这些值是从最初的值变化到临界值，说明了工作站想要传输时网络的整体问题。

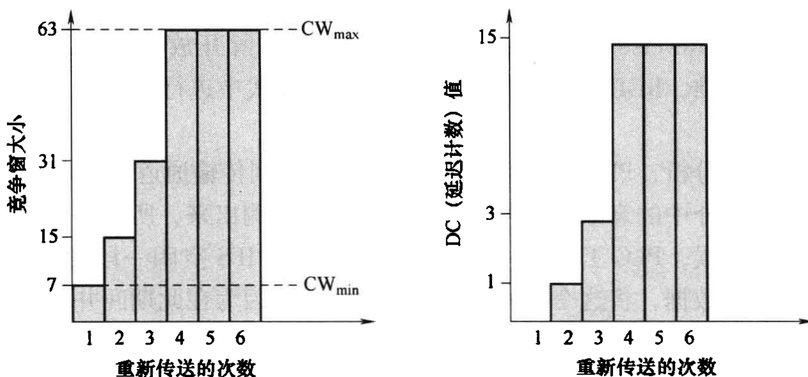


图 3.7　退避算法的竞争窗大小的变化

当媒介再次空闲时，并且在一个 CIFS 和帧优先级化的时长后，工作站确定媒介仍旧是空闲的，那么工作站将要递减计时器中的时隙个数，直至时隙递减完毕。如果此时媒介还是空闲的，那么该工作站将传输数据，并且禁止其他工作站接入媒介，从而封锁其计时器。

即使是在没有冲突的情况下仍可使用退避进程。一旦工作站检测到冲突或者是 BPC（退避进程计数器）为 0，该工作站就增加 BPC 值。在退避期间，如果有另外一个站先行进行传输，那么该工作站就检查它本身的 DC（延时计数器），并递减

它直至为0。在递减完DC后，工作站将它的计时器锁定在对应的BPC值上。

一旦工作站传输完毕，其他想要传输数据的工作站仍要等待一个CIFS和优先级化的阶段。在这期间它们检查媒介是否被占用，在CIFS之后，在上述锁定的时间计数器上继续递减，直至有其他工作站传输数据。但是，工作站不提取新的时间计数器的值，因为已经为接入媒介进行了等待，所以与刚开始尝试接入媒介的工作站相比，这些工作站接入媒介的可能性更大。

如果DC值为0，那么所有等待传输数据的工作站都必须经历一个退避进程，延迟它们的数据传输。

当计算计时器的值时，可能会有两个或者是更多的工作站会提取到相同的时间值，它们会在相同的时刻倒计时完毕，这样会导致媒介上的同步传输，产生冲突。因此，在退避进程完成之后，工作站为了新的传输，必要时就要重置退避算法，其中包含新的CW和DC的值。如果一个工作站接收到一个好的ACK信号，那么这些值将被重新设置到它们的最小值。

如果CW和DC的值均达到了HomePlug1.0标准定义的最大值，那么即使BPC在递减，CW和DC的值还是可以保持的。

如上所述，当使用退避算法时，同一网络中的工作站接入媒介的概率是相等的。这种算法的唯一缺点是不能保证一个最小时间。因此，在实时系统中，如语音、视频，使用退避算法是非常困难的。

HomePlug AV中TDMA和媒介接入

因为CSMA/CA算法并不能保证一个最小的传输时间，因此HomePlug AV标准作为HomePlug1.0的扩展，基于TDMA媒介接入系统增补了一个传输时隙的分配。

对在每一个工作站，TDMA媒介接入系统用于传输时间的确定性分配。这个分配是由CCo设备管理的，用来协调各个网络工作站对媒介的接入。

图3.8给出了TDMA复用技术中时间区域的划分情况。我们注意到，传输帧的时隙被划分为TDMA子块，恰好对应于两个工作站通信时长间隔。例如，在TDMA1子块中，仅仅只有工作站1和工作站2能够进行通信。这就保证了在PLC网络上进行通信的时间组织性。

因此，HomePlug AV定义了这个确定的时长，即基于信号过零同步的220V/50Hz的电信号的两个周期。这些TDMA时间区域被划分为几个确定和固定的时间分配。其中的一个时间分配是预留给CSMA/CA帧，帧交换遵从HomePlug 1.0和HomePlug AV标准。

数据传输举例

当一个信号源想要传输数据到终端时，必须确定媒介是空闲的。如果在相应的一个CIFS内没有侦听到任何活动，那么当信号源等待到一个优先级化时段时就可

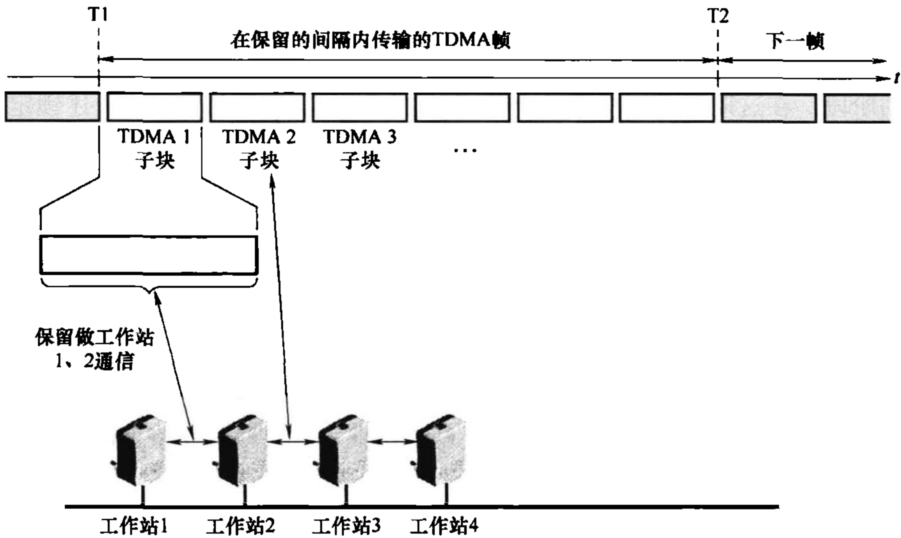


图 3.8 PLC 帧的时分多址间隔的时间划分

以进行数据传输。

图 3.9 表示在数据帧传输期间计时器的作用以及时间计数器值的获取。

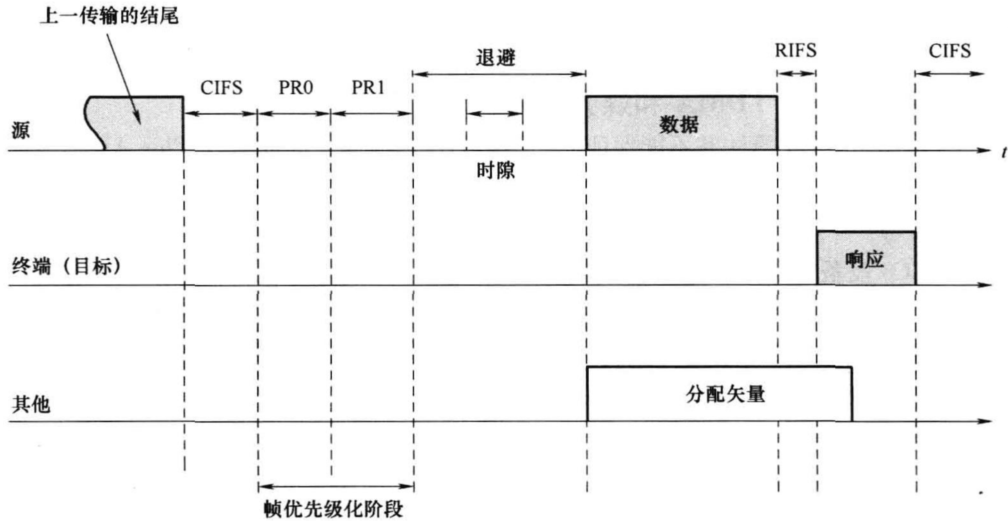


图 3.9 在数据传输时计时器的作用

如果媒介正处在工作状态，那么工作站将等待直至媒介空闲。一旦媒介空闲，工作站再等待一个 CIFS，确定媒介是空闲后，再次初始化退避算法以防发生冲突。当退避算法中计时器中的时间耗尽时，媒介仍旧是空闲，那么信号源就可以传输数据了。

当两个或者是多个工作站同时接入媒介就会发生冲突。在这种情况下，这些工

作站将重新使用退避算法接入媒介。如果数据成功被接收（这需要靠终端工作站检查数据帧的 CRC 来确认），那么这个终端工作站要等待一个 RIFS 时间间隔，然后发送 ACK 信号确认已经正确接收。

如果源工作站不能收到 ACK 信号，或者是数据不能够被正确接收，或者是 ACK 信号不能被正确接收，那么就可以假设有冲突发生，重传输进程就会被启动。

3.2.2 ARQ 进程

当源工作站在媒介中传输数据时，它要等待一个终端站发送的确认帧。未接收到或者是接收到错误数据而启动重传输程序，就叫做 ARQ（自动重复请求）。

终端能够重新发送 3 种类型的确认帧：

1）ACK。终端正确地接收到帧中的数据信息，并且这些数据信息是正确的。

2）NACK。终端正确地接收到数据，但是其中一些数据被破坏。这项检查是由 CRC（循环冗余校验）完成的。然后，终端发出请求，要求信号源重新发送被破坏的数据片段。

3）FAIL。数据没有发送到终端，或者是终端缓冲区已满，不能再接收和处理数据。

图 3.10 从时间的角度说明了 HomePlug 1.0 PLC 标准中各种类型的确认帧。通

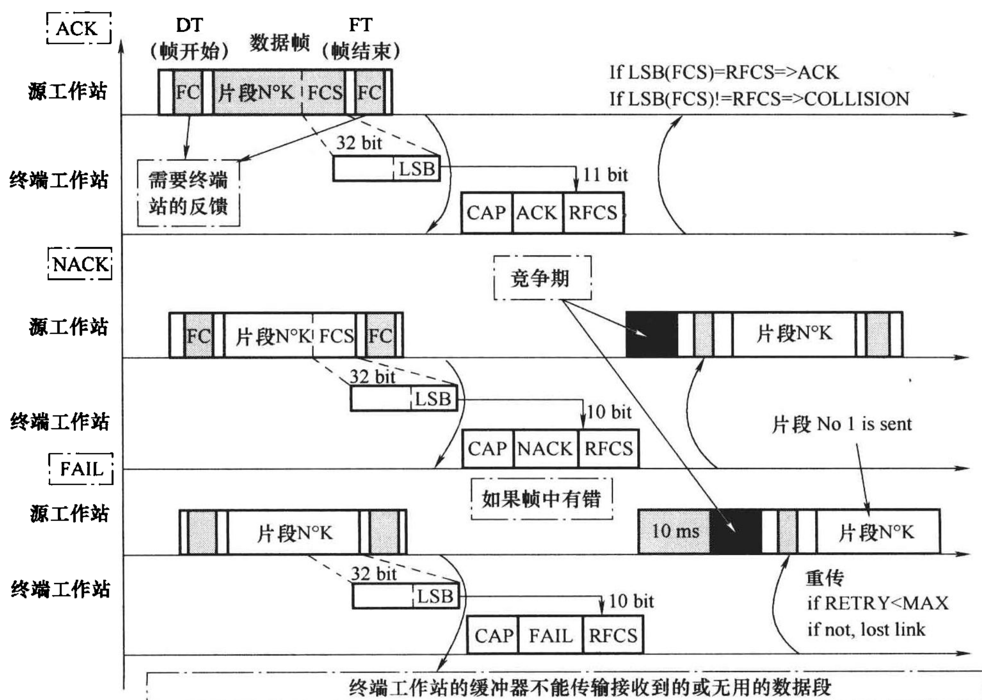


图 3.10 ARQ 进程中的确认帧

过允许信号源和终端之间的这种交换处理，大大提高了媒介接入的质量。

信号源和终端使用数据帧中的一块区域来鉴别那些将要回送至源工作站的响应帧，将这块区域定义为 FCS（帧校验序列），用于检查终端接收到的数据的完整性。

同样的方法，终端工作站使用这块区域的一部分（RFCS 区域，FCS 响应）重发确认信息。源工作站通过对比发送的 FCS 和接收到的 RFCS 来获知数据是否被正确接收（见图 3.11）。

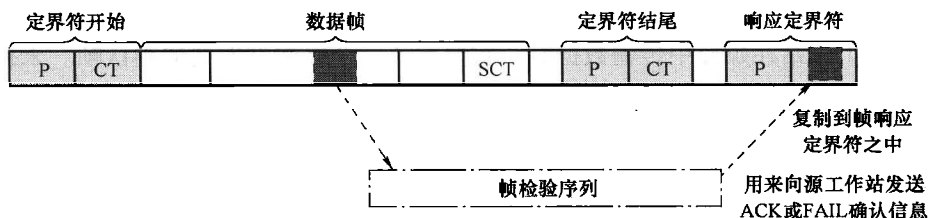


图 3.11 ARQ 进程中利用 FCS 和 RFCS 进行帧校验

ACK 响应

在 ACK 情形下，终端工作站重新发送一个包含源工作站传输的数据帧中的 RFCS 的响应帧给信号源。信号源利用这块区域获知数据是否被正确接收或者判断是否有影响数据传输的冲突发生。

图 3.12 描述了 HomePlug 1.0 标准中这种确认机制。

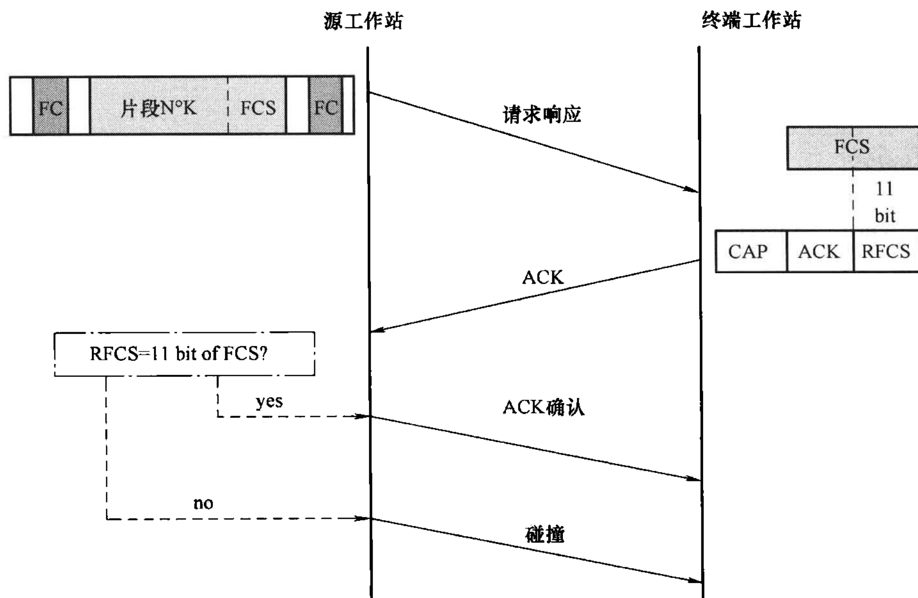


图 3.12 在 HomePlug 1.0 中应答式确认

NACK 响应

在 NACK 中，为了指出在传输过程中数据被破坏，终端工作站会在竞争周期之后重发给信号源一个响应帧。反过来，信号源会重新发送一个 NACK 信息和重新传输被破坏的数据片段（见图 3.13）。

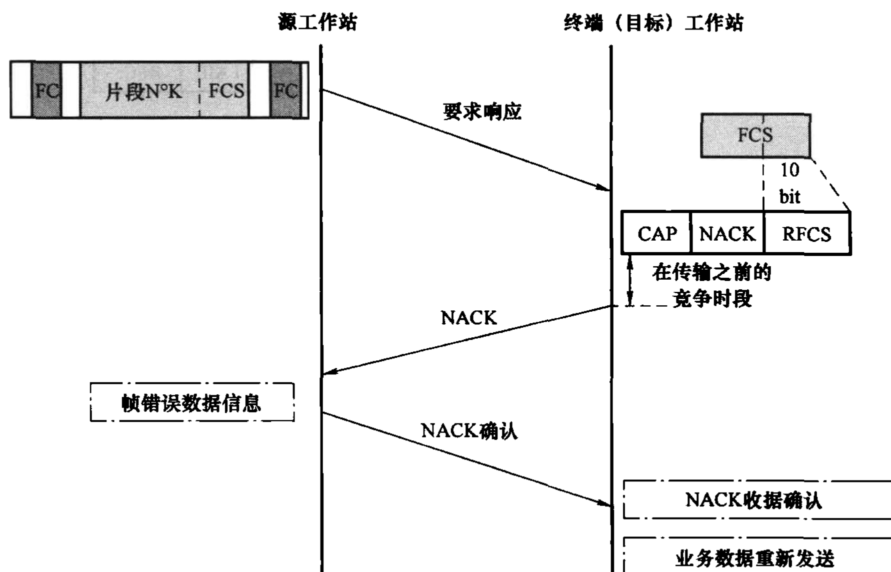


图 3.13 在 HomePlug 1.0 中非应答式确认

FAIL 响应

FAIL 响应表明，由于一个冲突或者是数据接收缓冲区的阻塞，终端不能使用接收到的数据帧。终端并不能预料它所能接收到的数据传输速率和所有接收到数据的存储情况。

在这一情形下，FAIL 响应竞争期强制规定为 10ms，如图 3.14 所示。

终端站记录了 FAIL 状态出现在片段中的次数。如果这个值超过了给定的门限值，那么终端站就会要求信号源从业务块第一片段重新发送服务模块。

HomePlug AV 中的 SACK 响应

在 HomePlug 标准的 AV 版本中，新加入了一个响应，即 SACK（选择性 ACK）。因为事实上，就有用的吞吐量而言，两工作站之间的 PLC 链路不一定是对称的。由于电力网络的特性，数据传输在各个方向上的影响是不一样的。SACK 响应被 PLC 网络的中心设备即 CCo 用于管理整个链路，换言之就是 CCo 管理网络中 PLC 工作站之间的各种链路，以及分配 TDMA 媒介接入技术帧结构中的传输时间。

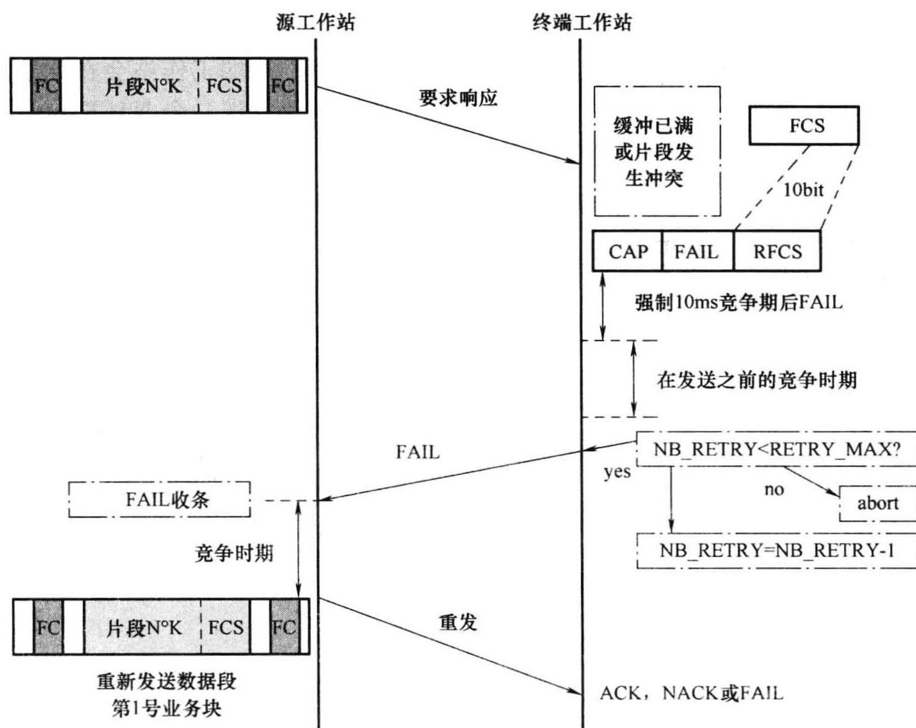


图 3.14 在 HomePlug 1.0 中失败响应

3.2.3 同步和帧控制

使用帧数据模块中的 FCS 区域检查帧。终端工作站利用这块区域发送合适的响应（ACK、NACK、FAIL）给源工作站。

源工作站使用响应帧中的 RFCS 区域检查这个响应的完整性，如图 3.15 所示。

终端工作站在一个帧间周期之后发送响应帧，通常这个帧间周期介于最小值 26μs 和最大值 1695μs 之间（见图 3.16）。因为定义的响应帧的长度小于数据帧，所以该响应帧能够被传输且不会占据太多的带宽。

HomePlug AV 帧同步

最新的 PLC 技术的发展，在保持 HomePlug 联盟先前版本中设备互操作性的同时，提高了设备的性能。PLC 技术组织的最新发展，直接促进了 HomePlug AV（音频和视频）规范出台的可能性，从而能够更有效地管理 QoS。

图 3.17 描述了 HomePlug AV 的信标帧（beacon frame）的组织形式。基于主-从结构模式，该标准使用 CSMA 和 TDMA 媒介接入功能。由于对媒介中数据通信而言，QoS 是最重要的（如 VoIP 中的实时数据流或者是 VoD 中的高速数据流），

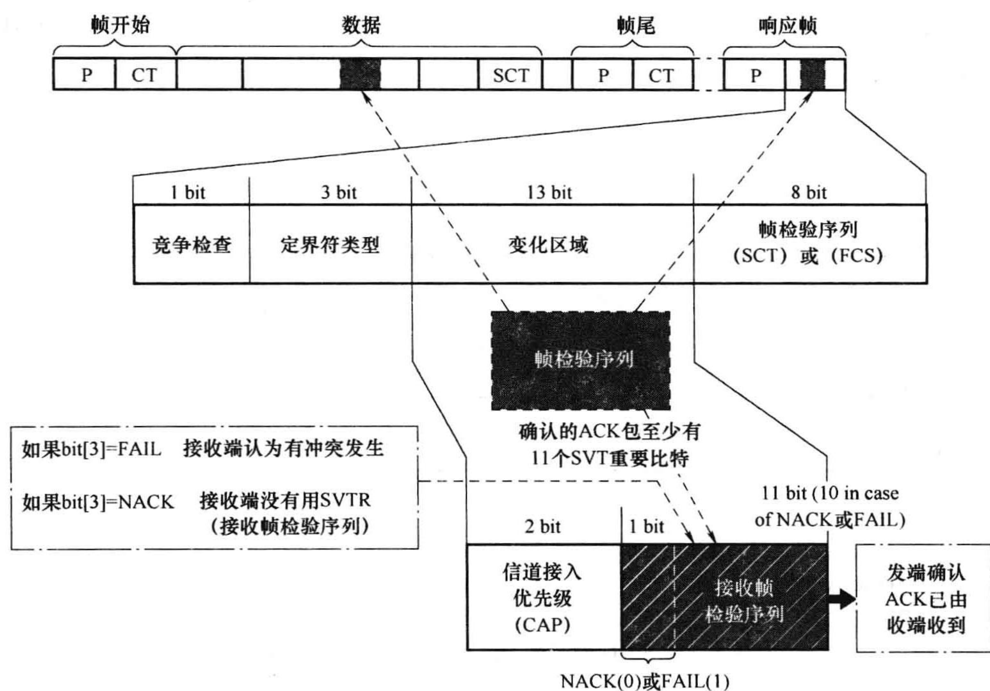


图 3.15 帧检查序列（FCS）

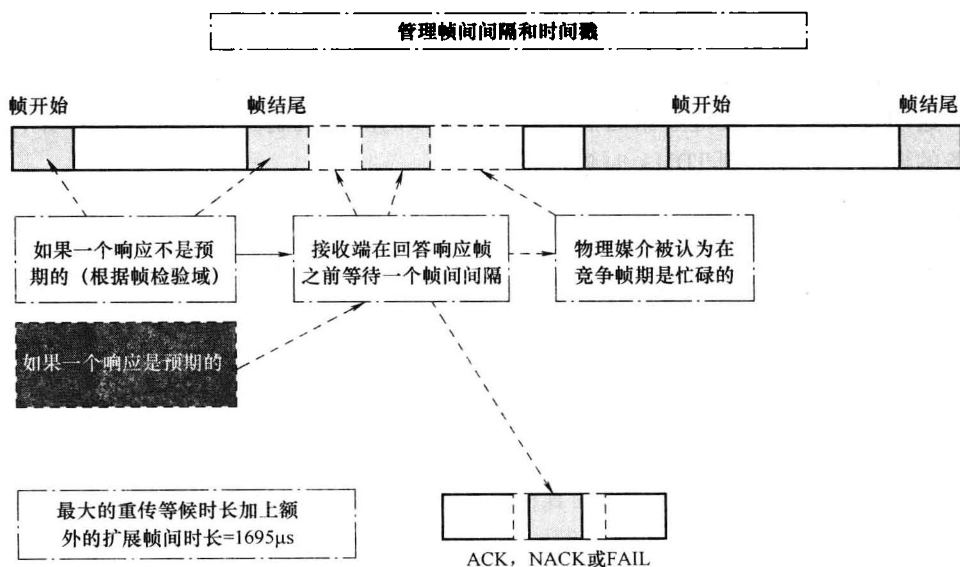


图 3.16 管理帧间间隔

CSMA 适用于那些媒介传输或者不区分优先级的数据业务，TDMA 适用于那些有优先级的数据的传输。

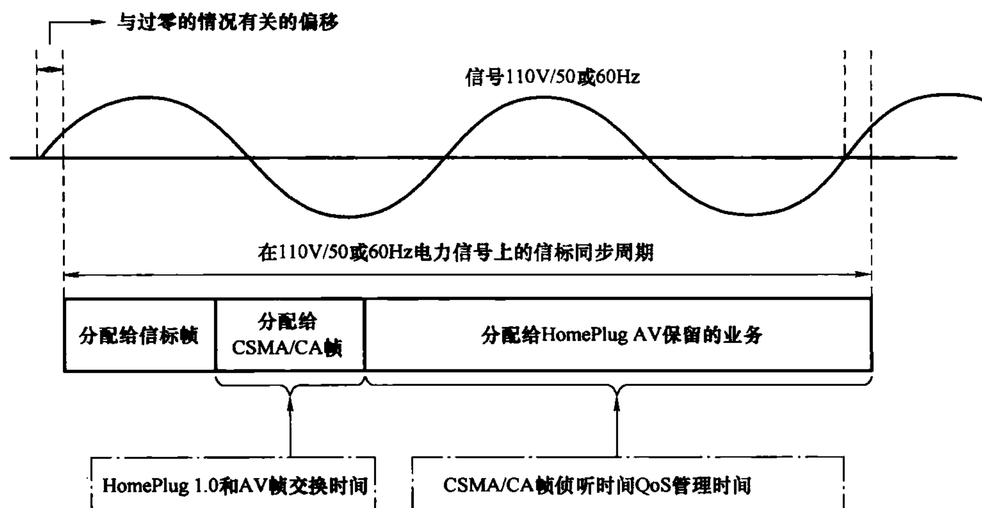


图 3.17　50Hz 信号的 HomePlugAV 信标帧同步

针对 PLC 技术，QoS 的管理通过一种非常有效的技术手段来实现，那就是在电力网络的 50 或 60Hz 的信号上实现同步的 TDMA 信标帧。由于，在整个公共电力网络和私有电力网络中所有这些确定性的信号是同步的。因此，无需借助一种专用的时钟，PLC 设备可以使用这样的 50 或 60Hz 的信号过零来实现同步。

这项技术包含了关键数据通信所需要的有效的决定机制。主设备根据网络中从设备的要求，对接入到 TDMA 时隙进行分配。

3.2.4　帧优先级管理

用来接入媒介的帧优先级由 CAP（Channel Access Priority，通道接入优先）区域和竞争窗（CW）的大小来实现管理。如图 3.18 所示。

就像在图 3.7 描绘的那样，CAP 变量影响着工作站接入媒介，图中，CW 和 DC 参数被退避进程设置，且数值由与网络中 PLC 设备各自的 CAP 值密切相关的表格给出。

PLC 工作站使用 CAP 变量通知其他工作站自己的媒介接入优先权。CAP 决定了数据帧优先权的 PRP1 和 PRP2 的值，该值被网络中的各工作站读取，以便确定各种优先权等级。这样一来，其他工作站便会被提前通知各个设备的优先等级。

整个过程称为 VCS（虚拟载波侦听），工作站在尝试接入媒介的过程中可以结合使用 PCS 和 VCS。

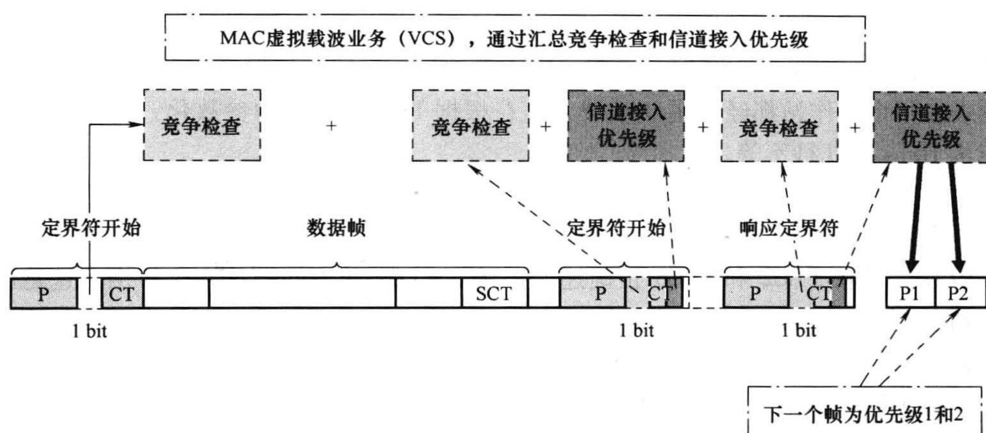


图 3.18 CAP（信道接入优先级）变量管理的帧优先级

3.2.5 频道（载波列表）管理

正如我们在上面所看到的，根据设备之间 PLC 链路的质量，存在几种不同的 OFDM 符号调制方式。在 Wi-Fi 中，每个工作站都能够设置它所希望传输的频道。与此不同，在 PLC 中，整个频带都被使用了。

图 3.19 描述了 4 个 PLC 工作站的简单网络。每个工作站都评估连接到其他 3

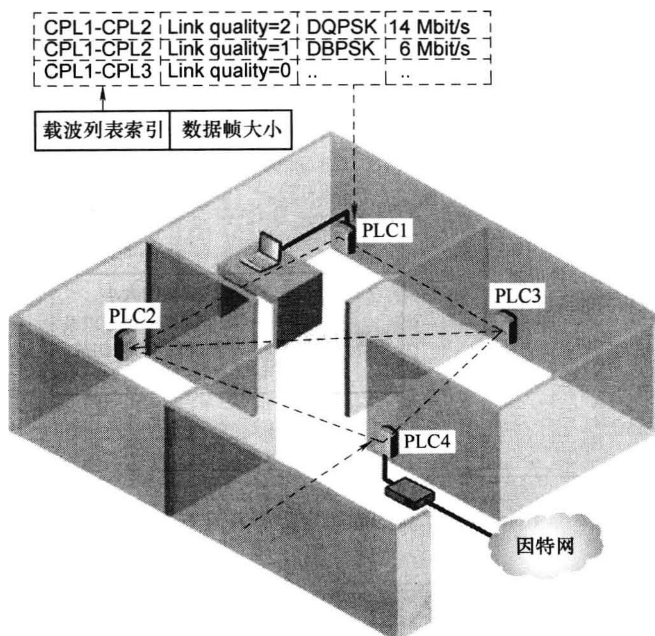


图 3.19 PLC 设备的载波列表管理

个工作站的 PLC 链路的质量，然后将信息存储在 PLC 设备的寄存器中的一个表格里面。这个寄存器可以通过一个起始帧定界符号的区域来访问，这个区域又称载波列表。每个工作站都经常更新载波列表；根据 PLC 工作站的参数化，更新时间可能从 10ms 到几秒不等。

一些工作站能够在 PLC 层看到彼此，但有时候其他的一些工作站却不能。设置一个工作站作为网关，使其能够看到所有参与的工作站很有必要。例如，在图 3.19 中，即便 PLC2 和 PLC3 正确连接，然而 PLC1 却不能够接入因特网，这是因为朝向 PLC4 方向的传输是不通的。如果电力线太长或者是电力网络太分散，那么将会导致 PLC 信号的衰减和恶化，从而无法实现更高层的数据通信。

图 3.20 说明了帧开始定界符的所有区域。在变化的区域，前 5 个比特用于载波列表。载波列表被用于存储朝向其他 15 个站的链路状态。这就决定了相同 PLC 网络中相关的 PLC 工作站数目的限制（HomePlug1.0 和 1.1 中为 16 个站；HomePlug AV 中为 250 个站）。还有一些数值是为 ROBO 模式或者为 HomePlug1.0 版本中特定应用所预留的。

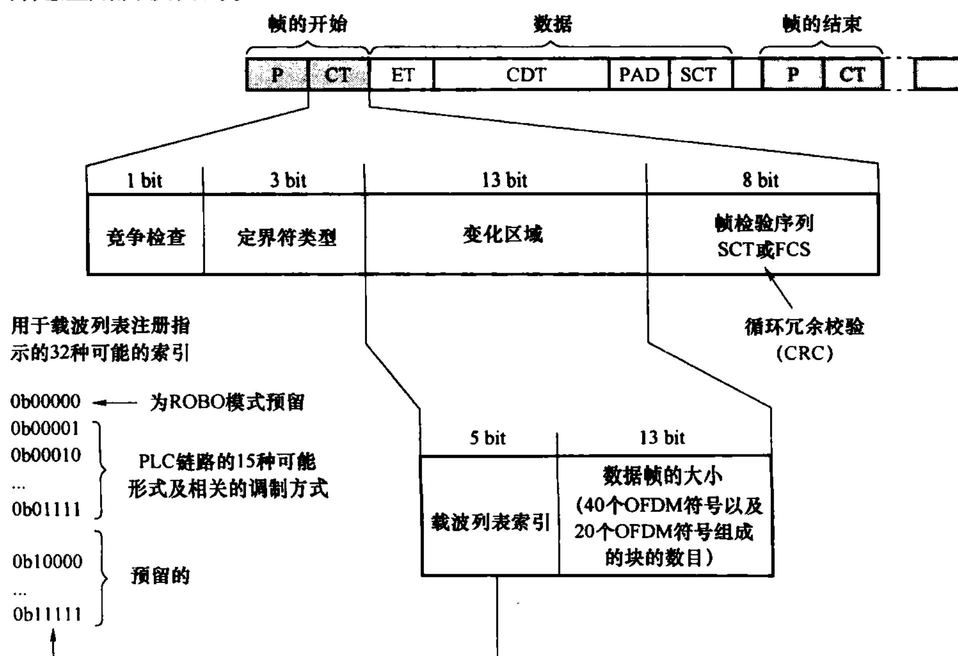


图 3.20 HomePlug 1.0 的起始定界符及其有关的载波列表

3.2.6 突发片段和无竞争接入

突发片段和无竞争接入是两种比较特殊的模式，两种方式旨在以更高的权限来

接入PLC网络以便能够发送连续的服务模块，而不需要在传输数据帧之前等待规定的CW。

在突发片段这种方式中，优先等级为CA3的PLC工作站将CC（竞争控制）设置为1之后，源工作站就可以发送两个连续的片段，而不需要再等待一个较高的竞争值。这种模式提高了性能，并且被证明对那些VoIP类型需要特殊优先级的应用而言十分有用。

图3.21阐述了突发片段的功能，能够使PLC设备以最大的优先级（CA3）传输一连串的业务块。

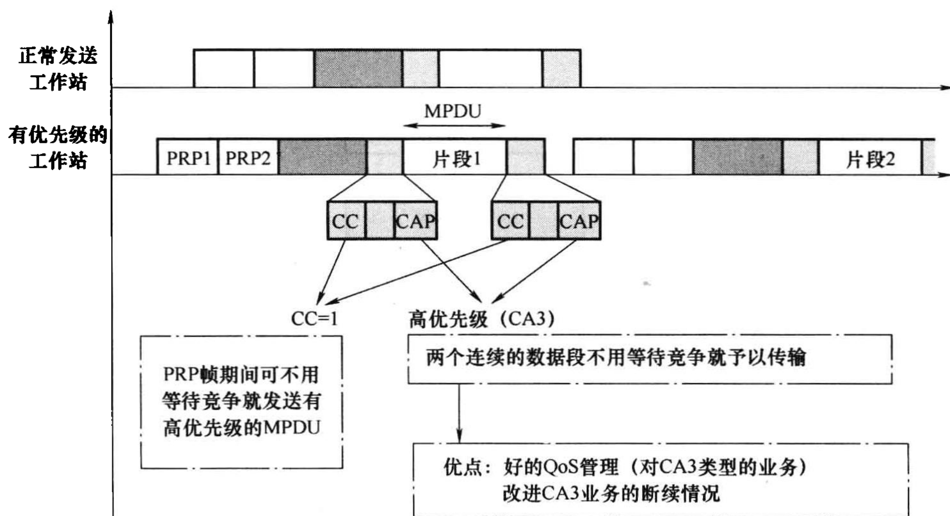


图3.21 突发片段模式管理

关于CFA（无竞争接入）这种方式，源工作站能够以优先级CA3发送所有的片段，通过设置CC=1，能够传送7个连续的MPDU。

3.3 帧等级功能

为了了解PLC技术的网络功能，需要掌握电力网络中传输的数据帧结构。

按照OSI模型，将网络分为7层，这就不难了解PLC技术中数据在每一个协议层是如何进行交换的。PLC技术仅在PHY层和MAC层起作用，因此它们从接口上看，可以看作IEEE802.3以太网。因此，网络工程师仅仅考虑IP、TCP，以及用户能够看到应用配置即可。

图3.22对比了OSI模型协议7层结构和PLC技术所在的位置。

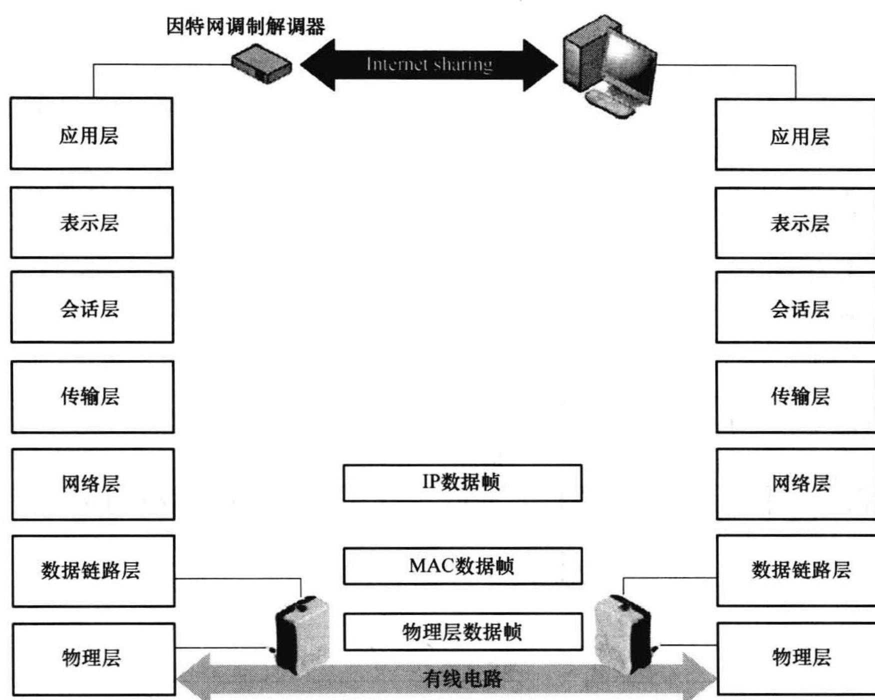


图 3.22　PLC 技术和 OSI 模型

3.3.1　MAC 封装

PLC 是 MAC 封装结构，而不像 Wi-Fi 技术协议层所采用的 IEEE802.11 架构。图 3.23 描述了 HomePlug1.0 PLC 架构的 MAC 封装。

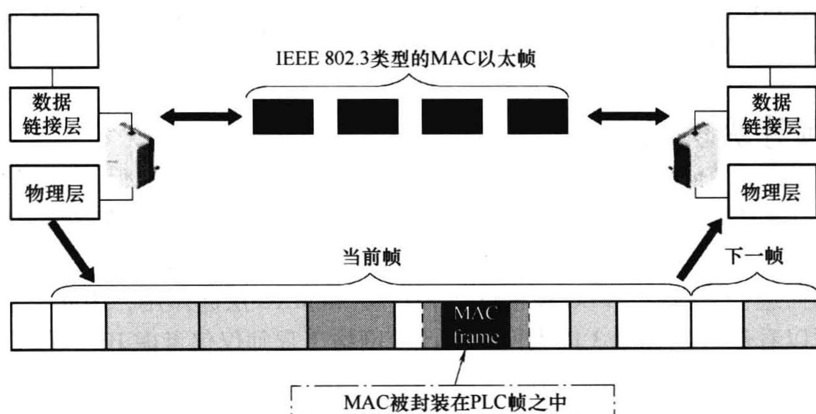


图 3.23　在 HomePlug 1.0 MAC 封装

从数据链路层角度来看，MAC 以太帧是对在 PLC 设备以太网接口处的物理帧解除封装之后而得到的。

3.3.2 分包重组

在 PLC 中使用共享媒介进行传输，往往会被那些用来专门传输数据的有线以太网线缆干扰，并且造成电力网络的误码率会很高（电力网络为 10^{-5}，以太网电缆为 10^{-9}）。

PLC 链路受到各种限制，比如干扰引起的衰减、电力线的多径效应，或者是电力线串音影响。这些限制会导致信号功率的衰减，从而不能保证数据的正确传送。

高的误码率会导致网络上所有发送错误数据的重新传输，这是以牺牲带宽为代价的，尤其是当发送数据很大时。

为了避免在很大程度上浪费带宽，PLC 技术使用了分包机制。在高噪声的环境中，它可以减少重传输的数据的数目。

分包

网络层（IP 等）或者是更高层的数据帧被数据链路层视为连续的 MPDUs（MAC 协议数据单元），形成 SB（数据块）。然后 SB 被划分为最大数据长度为 1500B 的片段。

因此，这些片段的大小为 1500B 或者是更少。在后一种情况下，片段将被填充到 1500B，目的是为了包含一个固定大小的 MPDU。在物理层中 1500B 与 160 个 OFDM 符号相对应。

将每一个组成 SB 的片段进行编号，以方便识别；这就为源工作站（MAC 层源地址）发送到终端工作站（终端地址）的 SB 信号重组提供了可能。

图 3.24 展示了不同的片段，这些片段由源工作站发送站、终端站进行编号。就像我们在 MAC 层看到的 ARQ 功能似的，如果 SB 片段中的一个没有被终端接收或者是接到的是被破坏的，那么将会首先在源工作站和终端工作站之间建立 NACK 或者 FAIL 响应，而不是首先重新发送遗失的或者是被破坏的片段。

重组

当终端工作站接收到片段之后，这些片段将会与工作站地址和优先权信息一起缓存和索引到终端工作站的重组缓冲区。一旦接收到所有的片段，数据块就会去封装，传送到 OSI 模型的更高层。之后，数据块就形成了以 TCP 或者 UDP 为帧头的 IP 帧。

然后，重组缓冲器清空，从而保证下一个帧的接收。缓冲区的大小能够被扩展到支持传输通道的最大传输速度。但是，由于接入到媒介的情况（CSMA）不是确定的，因此缓冲区不能预判数据片段的传输速度，只能自己寻找一个所谓的饱和状态。到达了这个饱和状态就不能再接收额外的数据片段。这时，终端工作站将要求

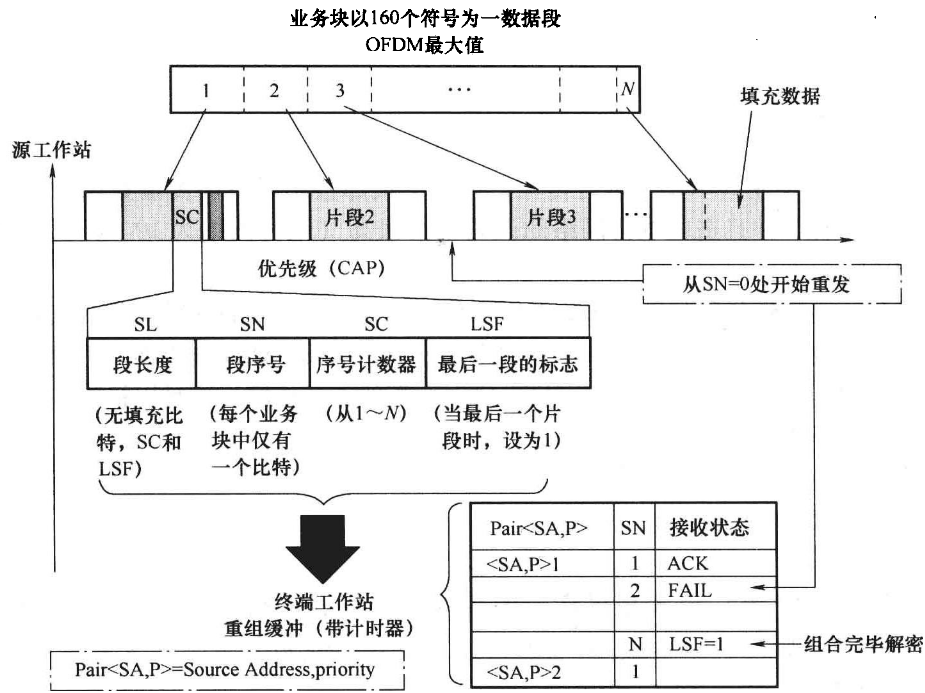


图 3.24　数据帧分段

源工作站稍后重新发送那些没有处理的数据片段。

3.4　其他功能

为了优化传输通道的使用，特别是在数据传输速率方面，PLC 采用了其他一些网络功能。这一功能的实现是根据 PLC 链路的质量，在物理层采用动态适应数据传输速率而实现的。

通过只向参与的 PLC 设备发送数据来实现整个带宽的优化利用。这些功能与其他网络技术的某些功能类似，例如 Wi-Fi。

3.4.1　比特率的动态适应

如上面指出，PLC 技术不停地在重新调整网络工作站之间的链路条件。

因为 PLC 链路取决于媒介条件，以及网络或引入的电力设备的干扰，所以对于 OFMA 符号形成的帧而言，要选择不同的调制方式来不停地调整传输速率。

对用户而言，动态连接到 PLC 网络终端之间的有用传输速率是随 PLC 链路而变化的。

表3.5列出了HomePlug1.0标准中PLC设备的各种传输速率或者是PHY传输速率。这个值是根据为每个工作站及其相关工作站而确定的载波列表得到的。

表3.5 HomePlug 1.0标准的动态速率

调制技术	编码参数	FEC（卷积码的编码率）	物理层传输速率/(Mbit/s)
DQPSK	23/39 ~ 238/254	3/4	14.1
DQPSK	23/39 ~ 238/254	1/2	9.1
DBPSK	23/39 ~ 238/254	3/4	4.5
ROBO（DBPSK）	31/39 ~ 43/51	1/2	0.9

3.4.2 单播、广播、组播

在PLC能够被看成是MAC封装技术的情况下，各种MAC帧发送的模式，不论是单播、广播还是组播都是允许的。

在单播模式中，一个网络工作站使用它的MAC地址发送数据给单一工作站。相比之下，在广播模式中，一个网络工作站使用专用于该模式的MAC地址发送数据给网络中所有的工作站，并且所有的比特数都为1。在组播模式中，一个网络工作站使用适用于整个工作站组的单一MAC地址发送数据给一组网络工作站。为了达到这个目的，必须提前定义与MAC地址相关的工作站组。组播MAC地址使用一个前缀作为它在网络中的身份。该前缀使用MAC地址的前48个比特。

第5章将说明，在MPDU数据帧的模块控制区域使用组播标志（为1bit）来支持广播和组播模式。

采取单播模式也是有可能的，这是因为PLC的辨识是通过它的MAC地址来确定的，如果一个工作站知道其他工作站的MAC地址，那么它就能够直接和独立地向该工作站发送MPDU。

3.4.3 服务质量

服务质量在IP网络中显得尤为重要，它主要用于区分网络中各种通信的优先权。第6章将会介绍，考虑到传输速率、网络传输时间和网络上传输的帧间抖动，IP服务需要不同的限制。

对于各种应用或者OSI模型高层来说，这些限制是决定性的。它旨在保持用于HTTP、FTP等的TCP连接。

因此，对于MAC层和物理层而言，根据高层应用的限制建立一个优先权等级是有必要的。在媒介作为MAC层网络集线器被共享的情况下，就必须在帧中建立这样一个优先权等级。

网络设备的优先权使PLC网络的服务质量成为可能。这些优先权由在竞争帧

之前的优先权（PRP1 和 PRP2）决定期间的 CAP 参数来表征。

图 3.25 描述了在 PRP1 和 PRP2 优先权决定期间优先权等级（CA0、CA1、CA2 和 CA3）。结束界定符和响应帧中的竞争比特是为了区分那些拥有相同优先级或者较低优先级的工作站的。

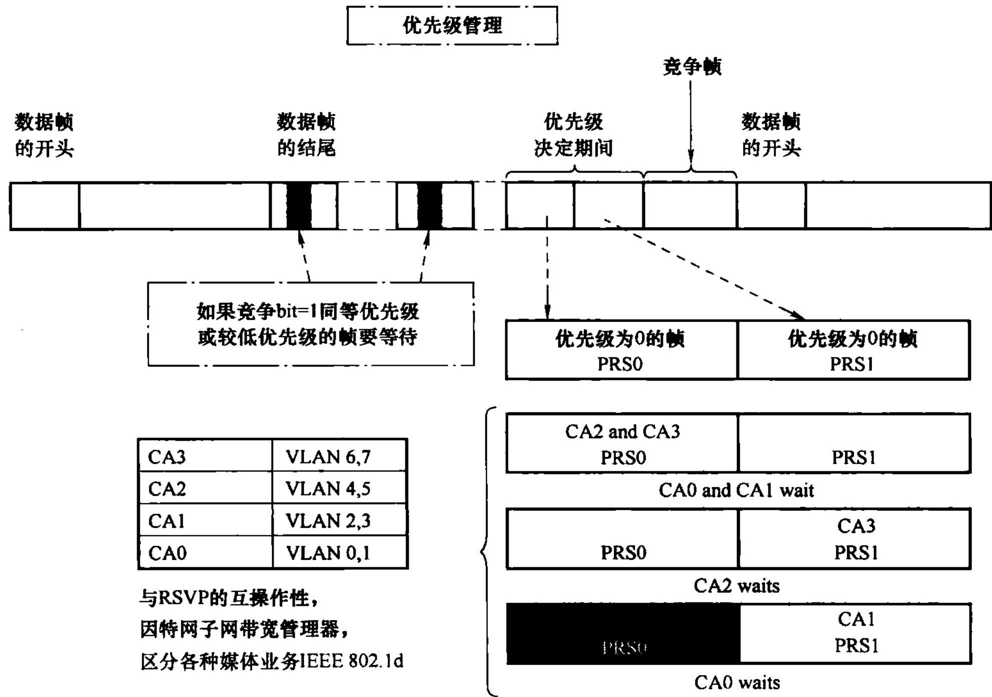


图 3.25 服务块的质量

使用 VLAN 标志

VLAN 标志主要是为了兼容 PLC 技术，因为这些标志就是用其数值来表征 PLC 工作站的 CAP 参数。

PLC 技术的优势之一是可以在一些 OSI 层建立虚拟网（比如 PLC 虚拟网、VLAN、MAC 叠加层等），从而为网络的综合功能提供更多的灵活性。

VLAN 标志可以实现一些 IP 数据业务和应用，特别是如下这些：RSVP（预约协议）、因特网子网带宽管理、区分各种多媒体业务、IEEE802.1D。

第4章 安　　全

在Wi-Fi网络中，安全是一个重要的问题。在PLC电路中，因为很难深入到物理介质中，所以安全问题很少被提及。Wi-Fi网络传输的介质是无线电，在无线电网络所覆盖的区域中，任何人都可能对其产生干扰，甚至是随意改变Wi-Fi网络的结构。虽然PLC中的电线是一种可以被各种网络设备共享的介质，由于存在着110或220V/50或60Hz交流电，所以想要接入其中是很困难的，并且是相当危险的。

因为电力网络的分布广泛，电力线路采取感性耦合或者容性耦合的方式将PLC信号传送至私人电力网络之外，这就从另一个角度表明需要采用具有相应安全性的软件。

现有PLC网络可以采取与固定有线高速网络相同的方式来确保安全。任何威胁都可以通过增加鉴权服务器和安全信道的方式来清除。

对于在内部网络推广IP电话的公司，安全是一个重大问题。在这样的背景下，就必须要有可靠的安全机制来防止窃听行为的发生。

4.1 网络安全概述

和其他网络相比，PLC可以避免一些类型的攻击，比如对PLC控制器的干扰和对传输信息的侦听。不过，PLC网络的优势来自于它所使用的传输介质——电线，这是因为对电线的接入十分困难，所以PLC网络在对抗攻击方面有特别之处。为了避免信息的泄露，网络传输必须对信息进行加密，确保任何不属于PLC逻辑网络的用户都不能续传和破译信息。

除了窃听信息之外，最主要的网络攻击莫过于那些旨在破坏网络的控制致使其崩溃或者旨在按照窃听者的意愿对网络结构进行重组。

对于所有这些攻击的防范措施就是使用密码、鉴权和真实性控制。密码的使用可以阻止入侵者接入网络进行数据交换；鉴权可以区分和识别任何想要使用网络发送数据的用户；真实性控制可以保证数据在传输过程中不被篡改。

4.1.1 加密

使用一种算法使消息难以分辨，这种方法并不新鲜。像埃及人、罗马人，早已开始运用各种方法来解密消息。这些相对简单的技术在不断演进。密码学在第二次世界大战期间已经发展成一门学科。

图 4.1 展示了密码学的基本原则。加密密钥用来加密明文，加密后的信息被传输给接收者，接收者使用解密密钥来重构信息。在传输过程中，一些人可以将加密的信息复原出来，采取不同的方式对其进行破译。



图 4.1 数据加密

密码学

加密系统包括加密设计和加密方法，试图破译已加密文字被称为密码分析，密码学就是研究加密系统和密码分析的学科。

在法国，对密钥的长度有着严格限制。最大长度为 40bit 的密钥可以被公众或私人使用。在私人使用时，密码的长度可达 128bit。如果长度超过了 128bit，密钥就必须传送到当地的网络安全主管部门。在美国或者日本，对于密码长度的规定是不同的，人们应当关注当地对密钥长度的规范。

有两种加密技术：一种为对称密钥算法；另一种为非对称密钥算法，更通俗的说法就是公钥加密算法。

对称密钥算法

对称密钥算法使用单独的密钥来加密和解密数据。所有希望安全传输数据的用户都必须共享一个秘密，那就是密钥。图 4.2 展示了处理过程。

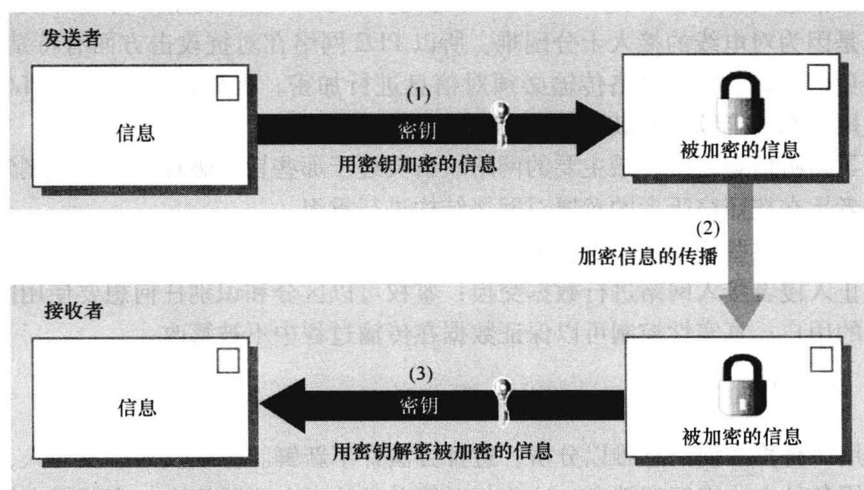


图 4.2 对称密钥加密

在这个系统中，有一个明显的漏洞：如何在发送者和接收者之间共享和传输密钥。

目前人们已经开发了多种对称密钥算法，例如 DES、RC2 ~ RC6 系列、AES（高级加密标准）等。

DES （数据加密标准）

DES 算法是由 IBM 公司和 NSA（美国国家安全局）合作开发的。DES 是一种“基于块”的加密算法。这个算法的密钥长度固定（40bit 或 56bit）。DES 算法的目的是通过在密钥和文本之间进行一系列代入与置换来加密信息的。

加密机制如下：

1）把需要加密的文本分成若干个 64bit 的块（block）（其中有 8bit 用于奇偶校验）。

2）对分割后的块进行初始置换。

3）每个块都分成两个部分，每部分 32bit，分别称为左部分和右部分。

4）对左右两个部分各进行 16 轮操作。每一次操作都包括对这个部分进行代入和置换，每轮操作都将数据和密钥进行混合。

5）16 轮操作结束置之后，将左右两个部分合并起来，然后对合并后的块进行逆向初始置换。

一旦所有的块都被加密，它们就会被重组以便产生加密文档，加密文档便在网络上传输。解密的时候也使用相同的密钥。

直到最近，DES 仍是对称密钥算法的参考方式，仍在多个系统中得到使用。例如，40bit 的 DES 算法被 SSL Internet v1.0 用于信息交换协议。

然而，因为担心 DES 算法过于简单，所以直到 1998 年才被使用。当前，它的加密算法已经得到了改进。

3-DES

3-DES 就是先后 3 次使用 DES。因此，数据信息将会通过使用 2 或 3 个不同的密钥来解密和加密。3-DES 密钥大约为 118bit。因此，在法国不能使用。3-DES被认为是安全合理的。

IDEA （国际数据加密算法）

IDEA 是一种密钥长度为 128bit 的算法。被加密的信息将被分为 4 块，对每个块进行 8 次循环加密。每次循环将分别“异或”操作，模 2^{16}和以及模 2^{16}乘这 3 个动作。在每次循环中，数据和密钥将被混合。这一技术使 IDEA 更加安全。

IDEA 在广泛使用的 PGP（Pretty Good Privacy）软件中得到使用。

RC2

RC2 算法是由 Ron Rivest 发明的，他把这种算法命名为 Ron's Code 2。该算法

基于块长度为64bit的数据块，密钥最大长度为2048bit，比DES算法快2~3倍。

该算法归RSA安全局所有，并在SSL v2.0中得到使用。

RC4

RC4不再使用块加密而是通过数据流加密。这个算法的特别之处在于对数据加密和解密采用了伪随机置换技术。

在RC4中定义了两种机制：

- KSA（密钥调度算法）。它由简单置换方式使用密钥生成一个密钥列表。
- PRGA（伪随机生成算法）。由KSA生成的状态表被置于伪随机数生成器（PRNG）中，PRNG将通过复杂的排列方式产生密钥流。

与其他算法不同，数据信息不用被分割成块来加密和解密。在RC4中，加密算法是把数据和密钥流进行“异或”操作，解密算法是把加密后的数据和相同的密钥流进行“异或”操作。

RC4的计算速度比RC2快。和RC2一样，该算法的所有权归RSA安全局。RC4算法在SSL v2.0和SSL v3.0中用于安全连接，也用于IEEE802.11系列标准中的WEP协议。

RC5和RC6

RC5的所有权依然归RSA安全局。RC5算法作为一种加密算法，它使用的块大小在32~128bit之间，循环的长度在0~255之间，动态密钥的长度在0~2040bit之间。

RC6是RC5的改进算法，因此其参数与RC5相同。唯一不同之处在于循环中增加了一个新的数学运算。

Blowfish

和DES算法一样，Blowfish算法应用于长度为64bit的数据块中。该算法基于DES，其密钥长度在40~448bit之间。这种算法速度快而且相当可靠。

Twofish

和Blowfish一样，Twofish加密算法的密钥算法长度可变，块大小为128bit，循环16次。这一算法可靠，并且速度快。

AES（高级加密标准）

AES算法诞生于NIST（美国国家标准与技术研究所）2000年发起的用于代替DES算法的研究项目中。在过去，AES算法看起来并不可靠。以前提出过多种算法，例如RC6和Twofish；但是因为速度快，算法可靠，最后Rijndael被接受，现在被命名为AES。

AES算法的块大小为128bit或16bit，密钥的长度可为128bit、192bit或256bit。依据密钥的大小，循环的次数可以为10次、12次或者14次。

在每次循环中，AES进行4项运算：

● 字节替换（SubBytes），在每个加密的数据块之中所使用的非线性替代（S）机制是不同的。

● 行位移变换（ShiftRows），转换块元素的置换（P）机制。

● 列混合变换（MixColumns），在不同的块元素之间进行相乘的变换（M）机制。块元素的相乘形式与传统的方式不同，采用的是 GF（2^8）的形式。

● 异或运算（AddRoundly），是一种密钥推导算法。它导致每次循环都有一个新的加密密钥 K*i*，其中，*i* 对应的是循环的次数。

数据信息在加密之前被分割成 128bit 的块。加密的第一步是把信息块和密钥进行“或”操作。然后，对每个信息块连续进行 10 次循环，每个循环都进行代替（S）、置换（P）和变换（M）操作。在每一次循环结束后，初始密钥产生一个新的加密密钥，变换（M）操作的结果与该密钥进行异或，所有这些结果进入下一次循环。在最后一个循环当中，不需要变换（M）操作，至此，数据块被加密。

一旦所有的信息块都被加密了，它们会被重组并生成加密信息，以便于在网络上传输。AES 加密的过程如图 4.3 所示。

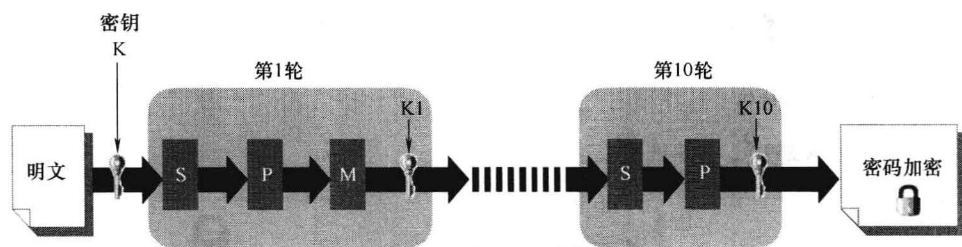


图 4.3 AES 加密

解密的过程与加密的过程相反，如图 4.4 所示。

AES 被美国管理部门用来代替 DES，也被 IEEE802.11 标准作为一种新的加密算法使用，以替代 RC4。

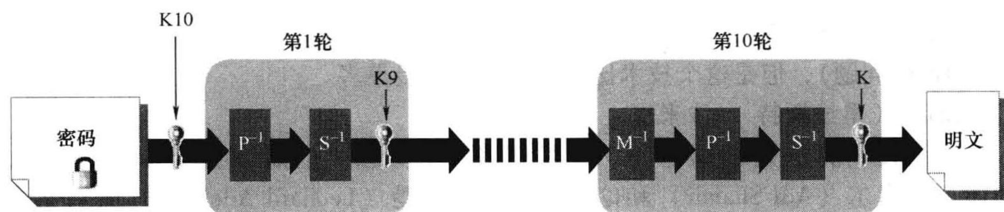


图 4.4 AES 解密

4.1.2 公共密钥算法

公共密钥算法要解决的是在传输过程中对称密钥的问题。

该算法中共有两种类型的密钥：

1）数据解密的私钥，这个密钥同样要保密。

2）对各个用户公开的公钥，这个密钥用于加密。

在两个密钥之间有一个数学关系，从其中一个密钥去推算另一个密钥是很困难的。

公钥以纯文本的形式在网络间传输，因此该文本需要加密。接收者利用自己的私钥要解密所收到的文本。处理过程如图 4.5 所示。

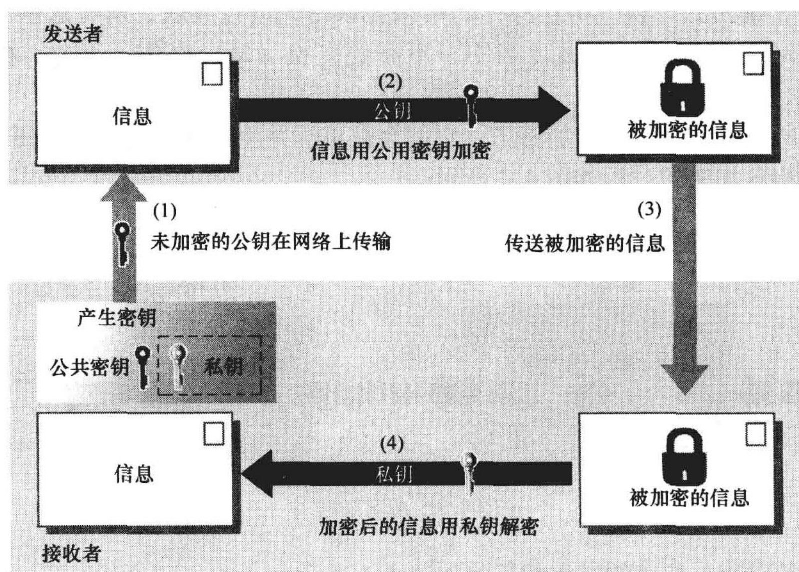


图 4.5 公钥密码

和对称密钥算法一样，公共密钥算法使用了不同的算法，特别是 RSA（Rivest, Shamir, Adelman）和 Diffie-Hellman。虽然这项技术弥补了对称密钥算法的不足（密钥传输问题），但是这个技术比对称密钥算法慢很多。

RSA（里维斯特、沙米尔、阿德尔曼）

这个公钥算法是根据它的 3 个发明者——罗恩·里斯维特（Ron Rivest）、阿迪·沙米尔（Adi Shamir）和伦纳德·阿德尔曼（Leonard Adelman）的名字命名的，于 1977 年被提出。这一算法主要用来处理大数据的因式分解所带来的困难。

RSA 使用密钥的长度不同，可以为 512bit、1024bit 和 2048bit。长度为 512bit

的密钥并不是非常可靠。不过，现在 RSA 还被用于 SSL、IPsec 和其他方面。在未来更好的数学算法出来之前，RSA 仍被认为是相当可靠的。

Diffie-Hellman

这是另外的一个公钥算法，它是由惠特菲尔德·迪菲（Whitfield Diffie）和马丁·赫尔曼（Martin Hellman）提出的。这是第一个被投入市场的加密算法。由于在某些类型的攻击面前显得很脆弱，因此最好在鉴权机构的帮助下使用。该算法的一个亮点便是两个人可以共享密钥而不用要求安全传输。直到今天，该算法仍在使用。

4.1.3 混合密钥算法

混合密钥算法（见图4.6）使用了前面所提到的两种技术，也就是对称密钥算法和公共密钥算法。它吸取两种算法的长处，弥补其中的不足。这些不足是众所周知的，例如对称算法不能保证密钥的传输安全，而公共密钥算法对数据加密的速度较慢。

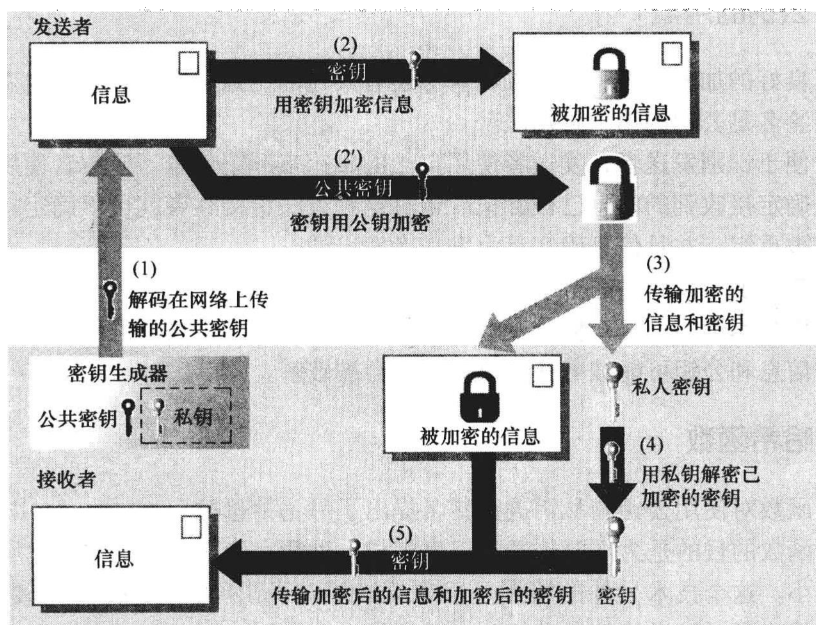


图4.6 混合密钥算法

在发送数据的时候，发送者使用对称密钥算法加密信息。与此同时，发送者利用接收者公共密钥算法的公钥对发送数据时使用的密钥进行加密，所以上述密钥就可以安全地在网络上进行传输了。

由于对称密钥算法的密钥长度有限，所以使用公共密钥算法对128bit的密钥进行加密速度是很快的。然后，加密信息传送给接收者，由接收者使用其私钥对加密后的密钥进行解密，从而解出发送者在发送数据使用的对称密钥算法的密钥。

这个技术的另外一个优点是在传给多个接收者的时候，不必再对信息进行多次加密。因为加密后的消息是与密钥一起传输的，你需要做的就是考虑采用不同的接收方的公钥对这个密钥进行加密。

4.1.4 电子签名

电子签名可以用来区别和鉴别数据发送者，它也可以用来检验网络上传输的数据是否发生改变。

多种技术都可以用来标记信息，公共密钥算法就是其中之一。但是哈希函数用得最多。

4.1.5 公钥的用法

除了良好的加密性能，公钥加密算法还有其他的优点可以对数据发送者进行鉴别，电子签名是公钥的第二种用法。

为了便于识别发送者，发送者使用自己的私钥来标记信息。接收者使用发送者的公钥来确定接收到的信息已被标记。通过这种方法，接收者就可以确定接收的信息有没有被重组，并且信息确实是由发送者发出的。

图4.7展示了该算法的整个过程。

虽然该技术确实可以对信息进行标记，但是加密性能却不能得到保证，因为加密之后的信息和公钥可能被截获，数据内容会被破解。

4.1.6 哈希函数

哈希函数对使用公钥和私钥进行签名提出了另一种选择。

哈希函数的目的是为需要传送的信息生成一种数字摘要，这个摘要比所要传输的消息要小。这个技术另外的特点是很难从摘要破译出原始信息，甚至是不可能的。这样就确保对发送的信息进行鉴权以及真实性鉴别。

图4.8描述了该方法的处理过程。发送者希望发送一组信息，并确保接收者能正确鉴权。为此哈希函数生成信息摘要，信息和摘要使用相同的哈希函数一起发往接收者，以便与接收到的摘要进行比对。如果摘要相同，这就意味着信息并没有被修改。

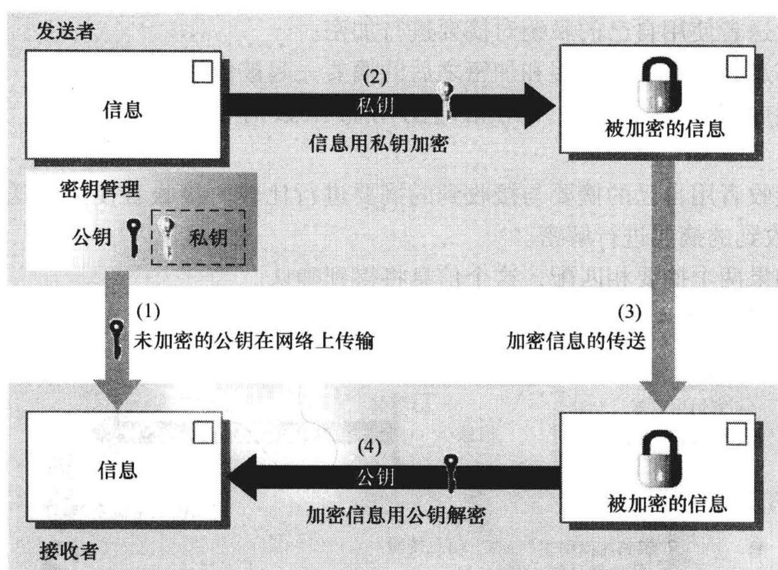


图4.7 公钥鉴权

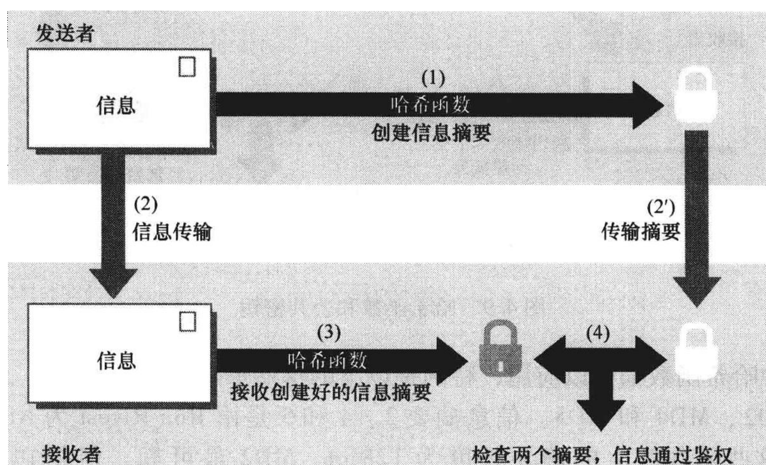


图4.8 用哈希函数处理信息

MD5

在因特网上，越来越多的文档和它们自己的摘要（通常是MD5）一起下载，来检查接收到的信息的真实性。

哈希函数经常与公钥加密算法合用，处理过程如下：

1）发送者使用哈希函数处理传输信息，生成摘要。

2）发送者使用自己的私钥对摘要进行加密。

3）信息与发送者的公钥和加密之后的摘要一起被传输到网络上。

4）接收者收到信息，并用相同的哈希函数对信息进行处理，重新生成摘要。

5）接收者用自己的摘要与接收到的摘要进行比较。接收者使用发送者提供的公钥对接收到的摘要进行解密。

6）如果两个摘要相匹配，这个信息将得到确认。

处理过程如图 4.9 所示。

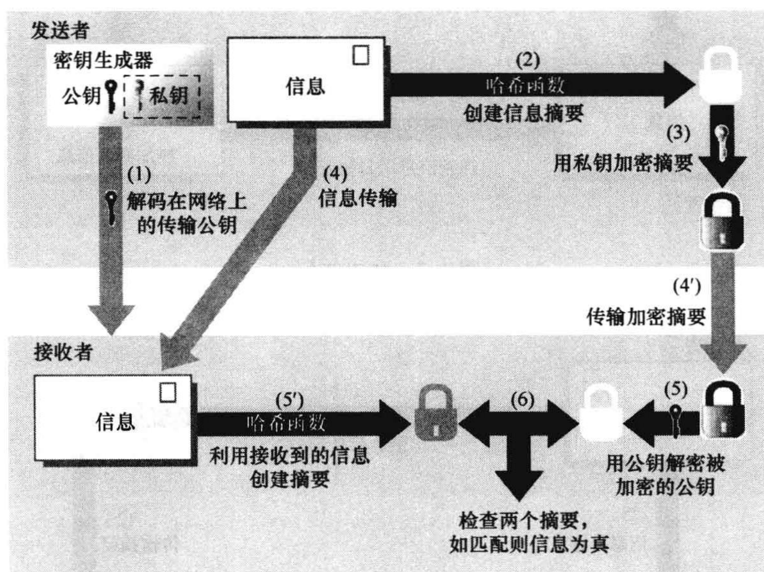


图 4.9 哈希函数和公共密钥

有多种哈希函数都得以应用，特别是以下的这些形式：

1）MD2、MD4 和 MD5。信息摘要 2、4 和 5 是由 Ron Rivest 为 RSA 安全局开发的。这些函数产生的摘要长度为 128bit。MD2 最可靠，但是它被优化为 8bit 形式，而另外两个为 32bit 形式。MD4 对确定攻击相当敏感，因此 MD4 被放弃使用了。MD5 是对 MD4 的升级。尽管 MD5 对确定攻击相当脆弱，但是 MD5 被认为是可靠的，且在多方面得到应用。在 RFC1321，MD5 被 IETF 确定为标准。

2）SHA 和 SHA1。SHA（安全哈希算法）和它的演进版本是由 NSA 开发的。两种算法所可以为高达 200 万 Tbit 的信息产生 160bit 的摘要。由于其摘要较大，因此很难受到攻击。攻克它的时间要比对 MD5 网络攻击的时间要长。

网络经常受到不同种类的攻击。有一些是消极攻击，例如为了截获信息而对网

络采取破解不同的密码和密钥来对网络进行监听。另外一些就是主动攻击。这些攻击者试图控制机器或者攻击其他机器设备。

经常出现的攻击如下：

1）拒绝服务（Denial of Service-DoS attack）攻击。这是最令人担心的攻击，这种攻击信息充满网络。这样一来，网络设备就不会再处理信息，有时候还会造成崩溃。

2）粗暴攻击（brute force attack）。这种攻击通过所有可能的组合进行尝试，以获得网络所使用的密码或者密钥。

3）字典攻击（dictionary attack）。这种攻击使用含有许多单词的数据库来尝试密码或者密钥。

4）欺骗攻击（spoofing attack）。这种攻击通过身份盗用来接入网络。它通过粗暴攻击或者字典攻击来获得某些信息，比如用户的登录和密码。

5）查询安全漏洞攻击。许多协议和控制系统因为设计原因而非常脆弱。这些漏洞既可被攻击者用来接入主机或者网络，也可以被用来控制主机或者重建数据。

6）病毒、蠕虫和木马攻击。这些攻击非常知名，它们可以破坏文件或者机器元件（病毒和蠕虫），也可能获得对主机的控制权或者窃取资源（木马攻击）。

4.2 PLC 网络安全

HomePlug 建立了一个基于加密密钥的 PLC 私人网络系统，其加密密钥由 PLC 设备控制，用来提高 PLC 网络的安全。

这个机制对网络管理者和使用各种具有相同逻辑网络的 PLC 设备的用户来说，安全、可靠并且注册简单。这些功能使 PLC 网络的发展更加简单。

PLC 设备在网络中注册的主要特点如下：

1）安全性。只有 PLC 设备拥有合适的密钥并且获得网络管理设备的授权和注册，才能在 PLC 网络中注册。必须能够便捷地将设备增添至 PLC 网络并且能够很方便地将设备从网络中移除。

2）可靠性。相同的 PLC 网络必须能够稳定地提供加密密钥配置并且以相同的方式来支持网络中的 PLC 设备的连接或断开。如果密钥丢失或者设备反安装，应当可以重建原始的结构。

3）简单。对网络管理者来说，管理不同 PLC 逻辑网络的密钥的过程应当简单。为此，HomePlug1.0 和 Turbo 定义了一个简单的密钥用来在网络对交换数据进行加密。复杂的 HomePlug AV 定义了多个网络密钥，这些密钥由网络的协调设备来集中管理。

因此，HomePlug 规定 PLC 逻辑网络基于一个叫 NEK（网络加密密钥）基础上的，对在不同 PLC 设备之间交互的数据进行加密（见图 4.10）。

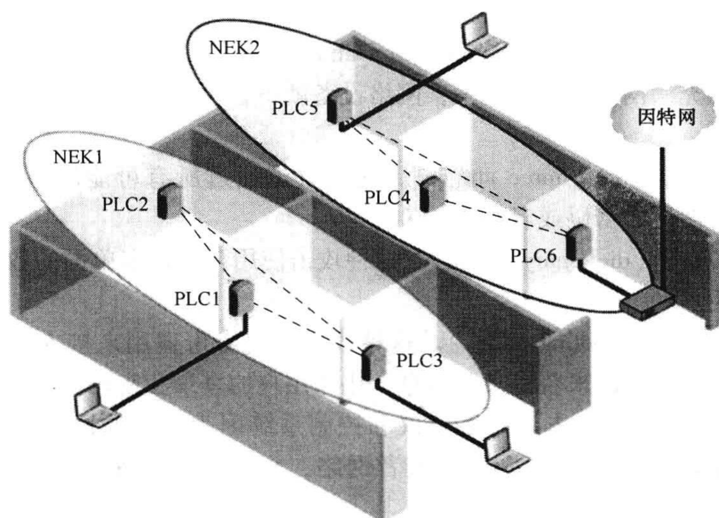


图 4.10 具有不同 NEK 的 PLC 逻辑网络

一个 PLC 网络可以通过多种方式来配置一个 NEK：

1）通过以太网接口。NEK 的帧结构通过一个配置工具，在 PLC 设备网络中进行广播。所有的 PLC 设备通过以太网接口这一手段来重建配置。

2）通过电力接口。NEK 的帧结构通过连接在 PLC 设备上的电力网络来发送。只有在知道另一个密钥即 DEK（默认加密密钥）的时候才能这样执行。这个密钥对每个 PLC 设备来说都是特定的。这个密钥是由设备制造商在生产设备的时候遵循 HomePlug 规范写入到设备内存中的。DEK 被配置设备和接收 NEK 的设备共同使用，以在电力网络上交互加密的 NEK。

3）通过 Web 接口。如果 PLC 设备功能更强，像美国 Asoka 公司的产品一样，密钥可以通过一个简单的 Web 接口来管理。

4.2.1 访问物理介质

在 Wi-Fi 网络中，传输介质是共享的。因此，任何在网络覆盖区域内的用户都可能按照自己的意愿拦截数据或者甚至重组网络。另外，如果一个不怀好意的人拥有的设备相当齐全，那么就算他不在这个覆盖范围内也能实现以上操作。这个人仅需使用天线（有无放大器均可）就能接入网络。

在 PLC 网络中，传输介质也是共享的，但是要想接入物理介质却是很困难的，而且具有潜在的危险。

然而，在PLC网络上的数据交换或多或少地使用了一些现有技术，特别是以下几项技术：

1）使用合适NEK密钥的PLC设备接入到目标网络。

2）依靠接近PLC网络中电力线路发射的电磁辐射来重建物理数据，但是这需要复杂并且昂贵的接收链。

3）生产特殊的PLC设备，可以重建出被加密的物理帧，以便于解密它们。

图4.11展示了拥有两个接口的PLC设备的内部设计：一方面，连接到传输不加密数据帧的与以太网相连接的以太网接口；另一方面，与传输加密数据的电力网络相连的PLC接口。

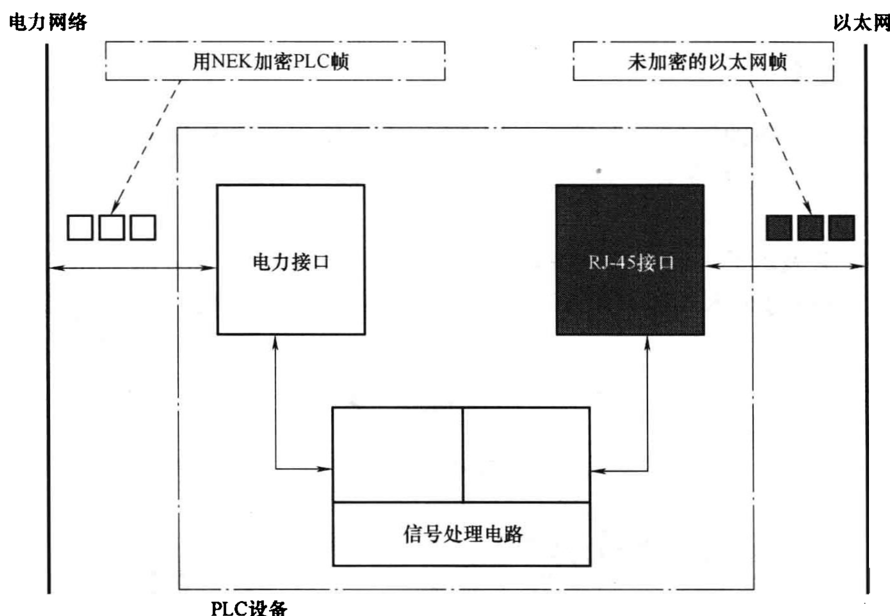


图4.11 加密交流帧的PLC设备的内部设计结构

一个PLC设备有一个可以在电力网络上收发数据帧的电气接口和一个可以在以太网上收发数据帧的以太网接口。在两个接口之间，如果设备拥有来自PLC网络的正确的NEK，数据才会传输。如果PLC设备没有NEK，以太网接口处将无法获得数据帧。因此，就无法轻易获得已经加密的PLC帧。

4.2.2 访问物理帧

在PLC网络中，传输的数据是由PLC帧承载的，被称为“物理帧”。

在电力网络中，PLC帧在各个插座之间以加密的形式传输。基于上面的叙述，接入物理介质很难。因此，这些帧实际上是被保护了起来，避免受到攻击，特别是

那些企图收集足够多的帧，从而采取暴力破解方法遍历全部组合或使用不同解密算法的那些攻击。

另外，PLC 帧使用多个频带进行传输；每个传输频带都会使用不同的传输技术，例如在信道中使用二进制数据调制技术。

正如我们在第 2 章和第 3 章看到的，各种 PLC 设备都会根据 PLC 连接的质量采取相适应的数据传输技术，例如传输信道所能承载的比特率。为此，tone map 记录了 PLC 设备之间的连接以及网络上的其他 PLC 设备情况，并加以保存。

为了接入物理帧，就需要时刻知道 tone map，以区别传输过程中所使用的不同技术。

4.2.3 鉴权

对 PLC 设备的鉴权主要就是获取 NEK（NEK 用来区分设备所属的网络）。如果一个 PLC 设备没有正确的 NEK，它就不能与相应的 PLC 网络进行数据交换。

图 4.12 展示了一个 PLC 设备通过识别 HomePlug1.0 和 Turbo 的 NEK 接入网络的过程。这里的 NEK（即“NEK2”）是 PLC 网络的识别工具，因为配备有这个网

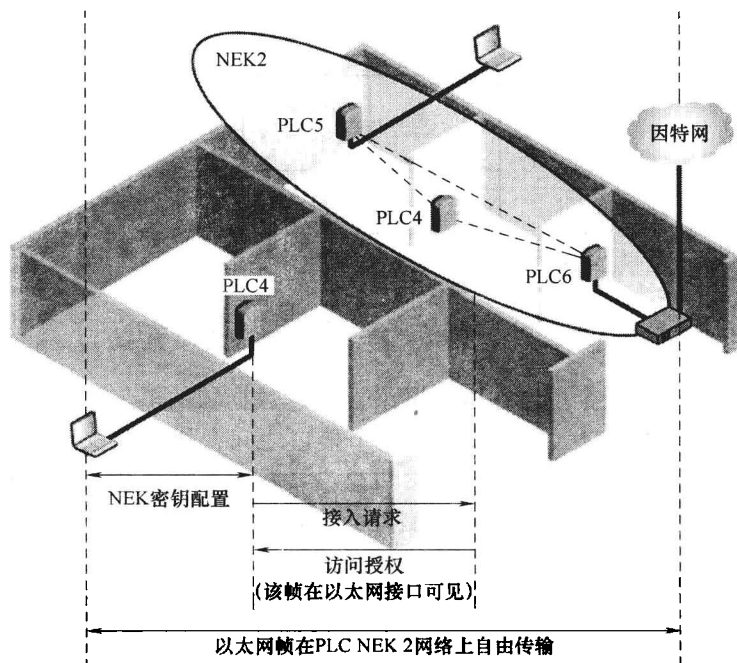


图 4.12 设备通过 NEK 密钥鉴权后接入 PLC 网络

络密钥的 PLC 设备才归属这个网络。

一些更为先进的 PLC 设备，如 Asoka 品牌的产品除了验证设备的 NEK 密钥还要对 MAC 地址进行鉴权。这个鉴权验证是在管理界面，通过一系列属于 PLC 网络的 MAC 地址进行管理而实现的。

4.2.4 网络密钥

在计算机网络中，网络密钥被用来保护交换数据。这些数据在传输之前已经完成了加密。在一个 PLC 网络中，数据在共享的电网中传输。因此，对数据进行加密是很重要的，以避免被破译。为此，PLC 网络使用密钥来辨别网络和属于该网络的设备。

HomePlug1.0 使用两个加密密钥，分别为 NEK 和 DEK。它们被保存到每一个设备的寄存器中，并且可通过修改 EKS（加密密钥选择）参数来进行访问。

WEP（Wired Equivalent Privacy，有线等效保密）被用来保护 Wi-Fi 网络中的数据，与此类似，NEK 以相同的方式鉴别 PLC 网络。NEK 用来完成以下工作：

1）在相同的电力网络上构建多个 PLC 网络。

2）对 PLC 设备之间传输的数据进行加密。

3）验证设备是否属于该 PLC 网络。

HomePlug PLC 网络的默认 NEK

在 HomePlug 中，默认的 NEK 等于 0x46D613E0F84A764C。任何在商店出售的 HomePlug PLC 设备都有这个加密密钥。

如果一个没有经过培训的人在毫无配置概念的时候使用这些设备，那么安全性将荡然无存。如果有数据在整栋大楼或者单独住所的电力网络中传输，所有设置为此默认 NEK 标准的设备所传输的数据都会被解密。

DEK 可以区别特定的 PLC 设备。通过建筑物或者商业应用场景中的电力网络，可以实现远程的 PLC 设备配置。这一密钥用来对持有 NEK 的 PLC 设备与企图加入本 PLC 网络的 PLC 设备之间的通信信息进行加密。在第 9 章我们将看到，特别是实际的 PLC 网络配置，利用这一密钥可以在网络管理中心处实现非常有用的 PLC 远程设备配置。

计算 NEK

PKCS#5 标准指定了两种使用密码加密的方法。在 HomePlug 中使用了 PBFDK1 方法。关于输入参数方面，它需要一个密码（由管理员输入）；一个“salt value”（这是一个公钥，由 HomePlug 指定固定的参数）；一个迭代计数（管理者在 PBFDK1 格式中指定了次数，将在一个循环中重复，以提高加密效率）以及还有输

出的生成密钥的长度。

PBFDK1 使用 MD5 哈希函数（对加密信息摘要的特殊定义和合成），在这里的目的就是用来加密信息和，以及用来生成 PLC 网络密码的数字摘要。该方法用方程描述如下：

$$DK = PBFDK1\ (P,\ S,\ c,\ dkLen)$$

其中，DK 为加密密钥（当 dkLen 为 8 时，DK 为 NEK）；P 为密码（由网络管理员输入）；S 是 salt value（等于二进制码 0x0885 6DAF 7CF5 8185）；c 是迭代次数（1000 次）；dkLen 为加密密钥的长度（8bit）。

根据 FIPS PUB112 标准，规定密码的长度为 4 ~ 8bit，甚至可能更长（如 24bit）。

PBFDK1 指定哈希函数（MD5）必须以迭代的方式执行 1000 次。第一个值是密码和 salt value 的级联。

迭代步骤如下：

$$T_1 = MD5\ (P \mid S)$$

$$T_2 = MD5\ (T_1)$$

$$\vdots$$

$$T_{1000} = MD5\ (T_{999})$$

$$DK = T_{1000} < 0 \cdots 7 >$$

其中（P | S）是 P 和 S 的级联。

MD5 算法（RFC 1321）

MD5 算法根据输入信息生成 128bit 的 MD（摘要）。在理论上，两个不同的信息不会产生相同的 MD。

MD5 算法如下：

$$m_{ext} = m + m_{pad} + m_1$$

其中，m_{ext}是由 MD5 算法生成的扩展信息；m 是自定长度的输入信息转变成一个数据流；m_{pad}是 m 之后的补足位（也就是 1 之后的若干个 0），将 m_{ext}补足为余数为 448（模 512）的长度；m_1是原始信息的长度，m 是 64bit 二进制块。

加长的信息 m_{ext}要经过 4 次变换，每次传输要经过 16 次处理。在每次处理中，都在上一次的结果上增加一个固定值。这个固定值是通过 SINE 函数计算出来的，被保存在一个 64 行 1 列的表格当中。

固定值的计算如下：

$addition = int\ (2^{32} \times abs\ (sin\ (i)))$

其中，i 代表随机数，这 64 个固定值（addition）将不会超过 32 位。

HomePlug AV 的安全性

在 HomePlug AV 应用的安全功能如下：

1）在密码段链接（Cipher Block Chaining，CBC）模式中用128bit的AES加密。

2）用一个NEK（每小时变换一个NEK数值）加密物理数据保护数据。

3）在网络上用NMK（Network Membership Key）来辨别NEK，在此NMK对进入网络的设备进行鉴权。

4）新的PLC设备通过以下配置来辨别：

◆ 在以太网接口上使用一个帧来传输NMK；
◆ 使用DAK（direct access key）代表HomePlug 1.0的DEK密钥；
◆ 使用一个简单的连接按钮；
◆ 使用MDAK（Meta DAK）；
◆ 使用一对PPK（Public-Private Key encryption）。

5）支持HLE（Higher Layer Entities）协议，例如IEEE 802.1x。

表4.1从4个方面总结了不同的PLC技术进行安全管理的特点：密钥管理、加密水平、优点和每个方法的缺点。

表4.1 PLC技术的密钥管理

技　术	密钥管理	加　密	优　点	缺点或不足
HomePlug 1.0	NEK	DES-56bit	简便	DES的不足 每个设备只有一个密钥
HomePlug Turbo	DEK	相同	相同	
HomePlug AV	NEK NMK DAK	AES-128bit （密钥轮转）	加密等级较高	使用快捷连接按钮时候存在弊端
Ascom	密钥交换	RC4 + Diffie-Hellman（128bit）	在接口处进行配置更加容易	RC4的缺点
DS2	主从密钥交换	3DES	由管理控制台对主设备进行中心配置	在鉴权期间，密钥可能被截获
Oxance	NEK DEK	DES（56bit） AES（128bit）	由Web中心接口进行管理	Web接口的相关缺点

4.2.5 攻击

正如我们在本章开头看到的那样，攻击的目的不是限制网络连接，而是为了从数据流中重建信息。攻击同时也企图打乱网络管理，既包括网络层，又包括物理层。

解密攻击

这个攻击的目的是发现PLC网络的NEK，以与PLC网络进行连接并且重建出

交换数据。以下两个技术用来发现 HomePlug 1.0 的 NEK：

1）需要访问物理帧并且保存足够的帧，以便于可以使用恰当的算法进行解密。但是这个技术非常复杂，并需要昂贵的、特定的硬件解决方案。

2）使用所有可能的 NEK 组合访问网络。

使用所有可能的 NEK 组合所需的时间，可以通过以下方法计算：PLC 网络用户输的密码（可能为 4～24 个字符）采用 56bit 的 DES 加密形成 NEK。

因此，所需尝试的最多次数为

$$N = 2^{58} \approx 2.88 \times 10^{17}$$

对于 100MHz 网卡接口的 64B 的以太网帧，传输时间是

$$T_{\text{frame}} = \frac{64 \times 8\text{bit}}{100 \times 1024 \times 1024} = 4.88 \times 10^{-6}\text{s}$$

那么遍历全部 NEK 组合的时间总共需要

$$T_{\text{total}} = N \times T_{\text{frame}} = 2.88 \times 10^{17} \times 4.88 \times 10^{-6} = 1.4 \times 10^{12}\text{s} = 44591 \text{ 年}$$

我们可以看出这个技术需要的时间太多，效率很低。

拒绝服务攻击

攻击的目的不一定要破解加密算法以重建出密钥，或者监听网络，或者接入网络。一些攻击的唯一目的就是通过组织网络管理来破坏网络。这种类型的攻击被称为拒绝服务攻击，或称作 DoS。这种类型的攻击在各种类型的网络中广泛存在。

在 PLC 网络中，最简单的拒绝服务攻击就是干扰。因为网络一般控制在 1～30MHz 的频带内，在 PLC 网络中的同一个频带内以更高的功率就会产生干扰，并且因此整体使用就受到限制；它甚至可以完全阻止网络管理。这个攻击应用起来是最简单的，不过它还不太容易控制。

4.3 IEEE 802.1x 和 PLC 网络安全的改进

IEEE 802.1x 是由 IEEE 委员会 802 小组提出的鉴权结构。这个结构并不是一个什么单独完整的协议，不过这些结构却指导着不同功能的定义，这里讲的功能就是指在本地局域网络（无论什么类型，例如以太网、PLC 网等）中设置用户鉴权服务器。

IEEE 802.1x 的结构被称作基于端口的网络访问控制，它基于两个要素：EAP（Extensive Authentication Protocol，可扩展鉴权协议）和 RADIUS（Remote Authentication Dial-In User Server，远程鉴权拨入用户服务器）协议。

端口在这个鉴权结构中扮演重要的角色。端口定义了局域网络结构中任意附属设备的类型。与以太网类似，在 PLC 网络中两个机器的连接便视作一个端口。

图 4.13 展示了 IEEE 802.1x 的结构。它包含了 3 个的元素：

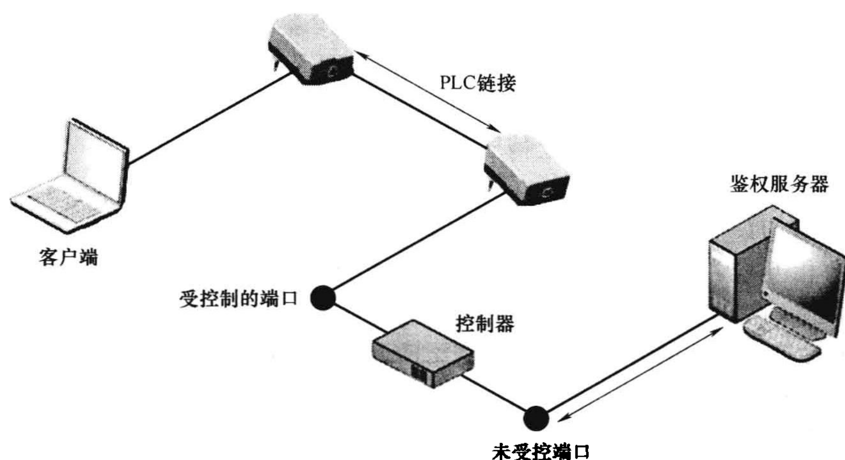


图4.13 IEEE 802.1x鉴权架构

1）一个客户端，它通过其他工作站接入网络。

2）一个控制器，通常是一个交换机或者路由器，它用来传递和控制在任何请求者和鉴权服务器之间的通信。

3）一个鉴权服务器，用来鉴权用户。

对于每一个端口，网络流量可能被监控也可能不被监控。在用户和控制器之间，端口被控制，从而确保端口中只传递着请求—回应类型的EAP鉴权信息。任何其他类型的数据都会被拒绝。相反，在控制者和鉴权服务器之间，传输介质被认为是安全的，所以任何类型的业务都会被接受。

在IEEE 802.1x中，鉴权是基于EAP和RADIUS的。

RADIUS和Diameter

IEEE 802.1x没有在服务器端定义特殊的鉴权协议。在客户端可以使用两种客户服务器鉴权协议，即RADIUS和Diameter。最简单的RADIUS已经成为所有IEEE 802.1x结构的默认服务器。Diameter的主要缺点是，它是基于SCTP（Stream Control Transmission Protocol，流控制传输协议）传输层的，并且在TCP层使用较少。

EAP

EAP原本是为PPP（点对点协议）定义的。它是现存的PAP（密码鉴权协议）和CHAP（口令握手鉴权协议）的扩展。与这两种协议相比，EAP提供多种简便的鉴权方法。因为EAP只是传输鉴权方法时的外壳，所以EAP才显得简单。

在 IEEE 802.1x 的 PLC 结构中，共有 5 种 EAP 鉴权方法：

1）EAP-MD5。这个方法是基于哈希函数（MD5）的。鉴权时，使用者提供一个登录密码，MD5 将该密码的摘要传输到想要鉴权的服务器。这个方法并不是很可靠的，虽然只有摘要在网络上传输而非登录密码。Windows XP SP1 并不支持此种方法。

2）EAP-TLS。TLS（传输层安全）是一个实施安全连接的方法。客户和服务器之间的相互鉴权，数据加密和动态密钥管理共同组成了它的功能。TLS 是 SSL3.0 的基础（在 HTTPS 中可以找到），是一个被许多网站（比如银行网站、在线预约网站等）使用的协议。除了加密，EAP-TLS 和 TLS 的特点相同，但是它们都被封装在 EAP 包中。

3）EAP-TTLS。EAP-TTLS（TLS 通道）是一种基于两个通道的 Funk 软件解决方案。第一个被用来采取 EAP-TLS 进行鉴权，第二个通道由制造商来选择确定鉴权方法（例如：EAP-MD5、PAP、CHAP 等），从而确保传输安全。

4）PEAP。PEAP 是一个由 Microsoft、RSA 和 Cisco Systems 提供的鉴权方法。和 EAP-TTLS 一样，PEAP 基于两个通道，但两个通道都用作 EAP-TLS 鉴权。

5）LEAP。又称轻量级的 EAP，是由 Cisco 提供的。它是一个轻量级的解决方案，但是具有相同的功能，如客户和服务器之间的相互鉴权，以及动态密钥管理。

虽然这些方法都是基于客户和服务器之间的相互鉴权的，但为安全传输数据的鉴权诸多方法本身并不是完美无瑕的。比如 MIN（Man In the Middle，中间人）攻击就可以在客户和服务器之间放入攻击者，解密信息和截获一个客户的鉴权，然后在当前位置鉴权攻击者。

综上所述，IEEE 802.1x 是一个采取增加管理 NEK 安全性的物理帧的方法，是提高 PLC 网络安全性的解决方案。

RADIUS

RADIUS 是集中用户鉴权和授权协议。最初是用于远程接入的，目前在许多环境下得到使用，例如 VPN 和 Wi-Fi 接入点，并且已经成为一个 IETF 标准（RFC2865）。

它在 ISO 结构位于 4 层之上，并使用了 UDP 传输协议，提升传输速度。它采用的是基于客户端—服务器结构。

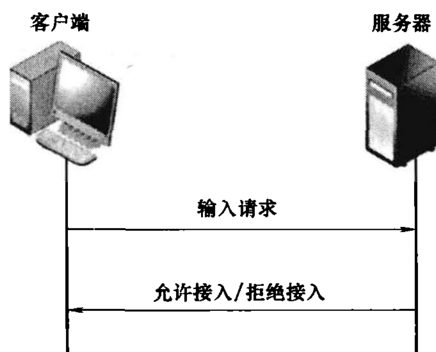


图 4.14 RADIUS 谈判

如图 4.14 所示，客户端发送服务器连接属性。服务器和客户之间的鉴权依靠共享的密钥进行，而这个密钥由一个密钥和

一些用户属性组成。鉴权时，服务器发送一个口令要求（challenge）给客户，只有掌握共享密钥者才能响应这个口令请求。RADIUS 检查客户发送的属性，并且检查对口令的响应，当属性和响应都无误时，将接受客户。

PLC 中的 IEEE 802.1x

EAPoL（EAP over LAN）是 EAP 的一个版本。这个版本在以太网和像 PLC 网络那样的 Wi-Fi 局域网中使用。从客户终端和 RADIUS 之间的连接角度看去，EAPoL 就是一个以太网的数据封装。图 4.15 展示了一个交换 EAPoL 信息实现对一个工作站的接入进行鉴权的过程。

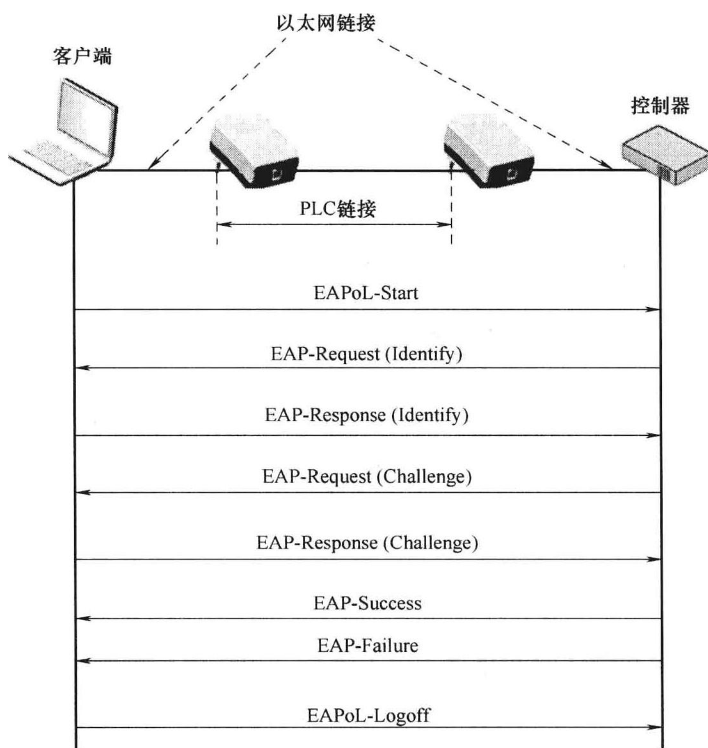


图 4.15　接入点和站点之间 EAPoL 的交互示意图

鉴权通常是由一个工作站发送 EAPoL-Start 要求来进行初始化的。接入点向工作站发去多个问询请求并且要求其必须回答。当接收到确认工作站被鉴权的 EAP-Success 信息或者有 EAP-Failure 信息时，鉴权阶段结束。当收到 EAP-Failure 信息时，鉴权失败。工作站随时都可以发送 EAPoL-Logoff 请求，这意味着工作站撤销鉴权。

如图 4.16 所示，IEEE 802.1x 使用鉴权服务器，其中由接入点来转发信息。

鉴权阶段只能被工作站初始化。在收到鉴权要求之后，接入点请求工作站使用一个 EAP- Request 验证自己（身份验证）。当工作站根据该请求在接入点使用 EAP- Request 验证自己之后，这个请求被传送到鉴权服务器（接入请求）。

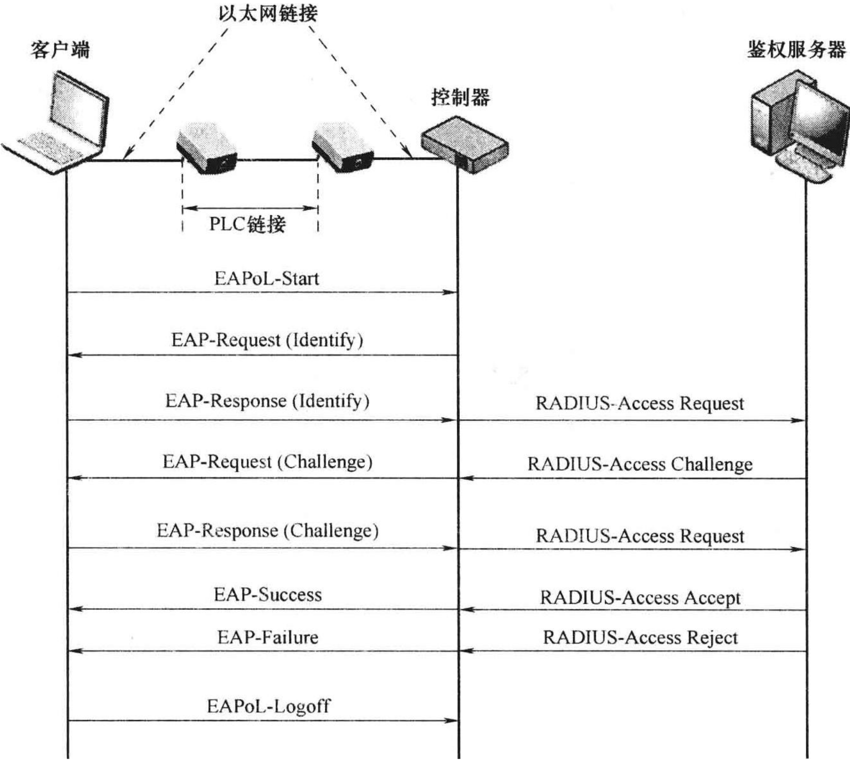


图 4.16　IEEE 802.1x 的鉴权过程

通常，工作站和鉴权服务器共享一个秘密（由使用不同的鉴权方法确定，包括密钥、密码、证书）。当鉴权服务器收到来自于连接在 PLC 网络上的客户发送来的请求时，它就发送包含问询工作站的接入口令信息。这个问询只能由工作站和鉴权服务器所共享的密钥解决。如果这个接入口令信息没有被解决，工作站就不能验证自己；如果口令正确，鉴权服务器就会验证工作站。此时，工作站就可以通过它与已经接入 PLC 局域网络的 PLC 设备之间的控制端口进入网络。

尽管任何类型的支持 EAPoL 的服务器都可以被用做鉴权服务器，但使用最广泛的还是 RADIUS。

虚拟个人网络

虚拟个人网络（VPN）为客户和服务器之间提供了一个端到端的安全隧道。VPN 用来辨别和鉴权，以便加密网络传输的任意数据流。

对数据来说，IPsec 是在 VPN 中最常使用的协议。前面曾经提到的 IPsec 标准根据不同安全等级的需求，采用的协议和算法是不同的：

1）由公钥电子签名（RSA）进行鉴权；

2）由哈希函数（MD5）控制真实性；

3）由对称算法加密，如 DES、3DES、AES、IDEA、Blowfish 等。

使用 VPN 是保护无线网络的最可靠的方法，这个方法也是最常用的。

第5章 帧

为了传输信息，PLC 工作站必须准备数据帧，也就是带有帧头以及帧尾区域的数据模块。包含用户数据的模块所具有的特殊格式，取决于接入物理媒介所采用的技术。由于电力线媒介是共享的，因此要考虑使用一种技术来传输来自不同设备的多个帧。在物理层上传输的帧是一种双层的结构，也就是第二层帧结构封装到第一层帧结构之中。

如图 5.1 所示，PLC 的数据通过 MAC 层（数据链路层）和物理层传输。第一层的结构与接入电力线媒介的技术相对应，与这一协议相对应的帧称作 MAC 帧或者 MPDU（MAC 协议数据单元）帧。

来自于 MAC 层之上的所有数据被封装到 MAC 帧里。为了通过物理接口或电力接口来传输帧，MAC 帧被封装到第二个物理层帧之中，这个帧称为 PPDU（物理协议数据单元）。

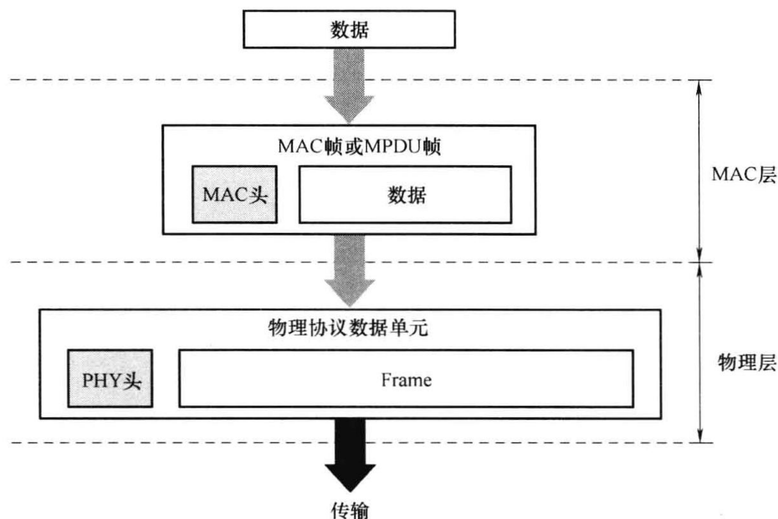


图 5.1　PLC 接入结构的数据传输过程

本章将主要介绍 HomePlug 1.0 的 PLC 帧结构，同时介绍 HomePlug AV 帧的主要特征。

5.1　物理层帧

如果观察一下 PLC 设备之间不断传输的 HomePlug 1.0 的物理层帧的完整结构（见图 5.2），就会发现，从 OSI 模型的角度来看，物理层帧之中围绕着长数据帧（这个长数据帧中包含着上一层的数据）有着许多组成的部分。

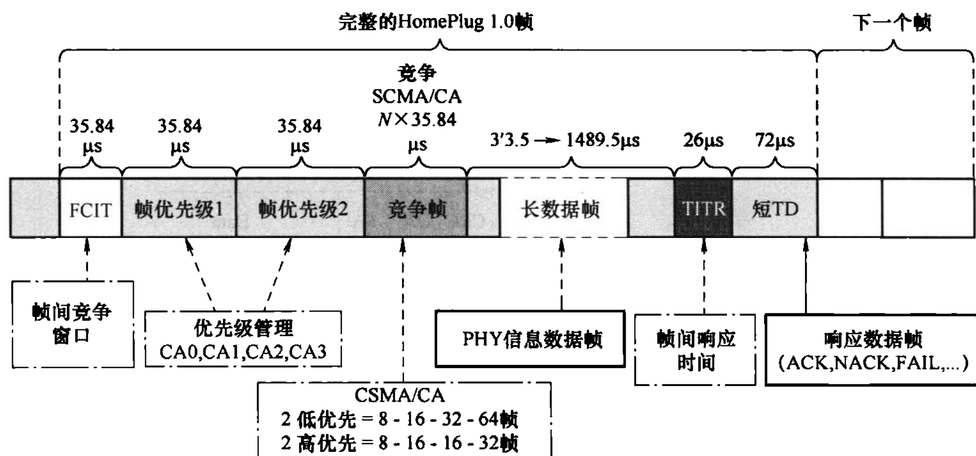


图 5.2　HomePlug1.0 的帧结构

从时间角度来看，HomePlug 1.0 帧由最小值和最大值来量化。帧结构中包含一个固定部分（也称帧头）、一个变化数据部分、一个与 CSMA/CA 过程有关的竞争时期部分，见表 5.1。

表 5.1　HomePlug 1.0 帧时长

固定部分（帧头）			变化部分（数据）		竞争部分（CSMA/CA）		时　长
最小	205.52μs	+	313.5μs	+	N×35.84μs	=	519.02μs+(N×35.84μs)
最大	205.52μs	+	1489.5μs	+	N×35.84μs	=	1692.02μs+(N×35.84μs)

因此，我们可以说，HomePlug1.0 帧之中包含着一个“长数据帧”部分，这个部分主要是 MAC 帧数据，还有一个“短数据帧”部分，这一部分主要包含了获得的其他 PLC 设备的信息。

需要指出，HomePlug 1.0 帧的平均时间是 1600μs。

从物理层调制角度的技术来看，HomePlug 1.0 数据帧包含 OFDM（正交频分复用）符号。这些符号构成一个个的块，最终构成了完整的帧。

图 5.3 表示这些不同的 OFDM 块各自占据的时长。

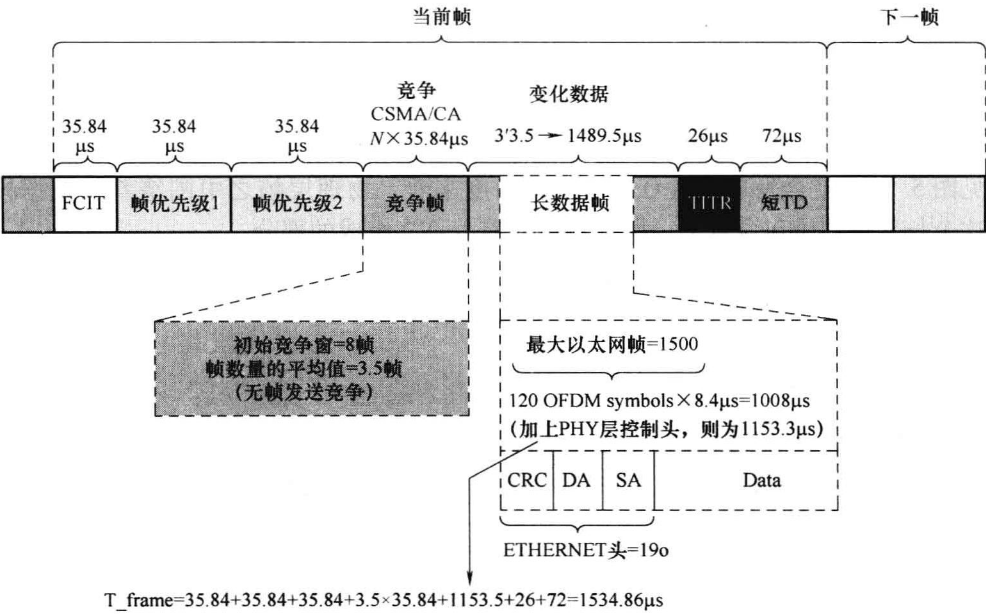


图 5.3 完整的 HomePlug1.0 帧结中的 OFDM 符号块的时长

完整的帧时长时就是将不同 OFDM 符号模块的时长相加。考虑到数据链路层，最大的可能传输速率如下计算。

要传输一个 2705B 的帧，最大传输速率可以用以下算式来计算，即

$$\text{Bit rate}_{\text{PHY_MAX}} = 2705 \times 8\text{bit}/1534.86\mu\text{s} = 14.1\text{Mbit/s}$$

传输一个最大长度是 1500B 的以太网数据帧，最大传输速率的计算式为

$$\text{Bit rate}_{\text{PHY_MAX}} = 1500 \times 8\text{bit}/1534.86\mu\text{s} = 7.81\text{Mbit/s}$$

表 5.2 总结了 HomePlug 1.0 标准的最大理论传输速率。正如我们在书中第 2 部分看到的，这些值比实际值要低。

表 5.2 不同调制技术的最大传输速率

模　式	纠错码（FEC）	理论最大传输速率/(Mbit/s)
DQPSK 3/4	3/4 卷积码和 R-S（Reed-Solomon）码	14.1
DQPSK 1/2	1/2 卷积码和 R-S（Reed-Solomon）码	9.19
DBPSK	卷积码和 R-S（Reed-Solomon）码	4.59
ROBO（DBPSK1/2，每 bit 重复 4 次）	1/2 卷积码和 R-S（Reed-Solomon）码	1.02

见表 5.3，随着 PLC 技术的发展，可以预计传输速率将进一步提高。

表 5.3　不同 PLC 技术的最大传输速率的预测

PLC 技术	传输速率预测/(Mbit/s)
HomePlug Turbo	85
HomePlug AV	200
Spidcom SPC200-e	220
DS2	200

HomePlug AV 物理层和数据链路层的结构

HomePlug 家族的最新技术进步使得 Homeplug1.0 的性能通过新版本的 HomePlug AV 得到提升。

物理层结构和数据链路层的结构已经得到了改善，允许了 HomePlug1.0 设备的交互，实现了主从模式。

图 5.4 说明了这两个层的结构。

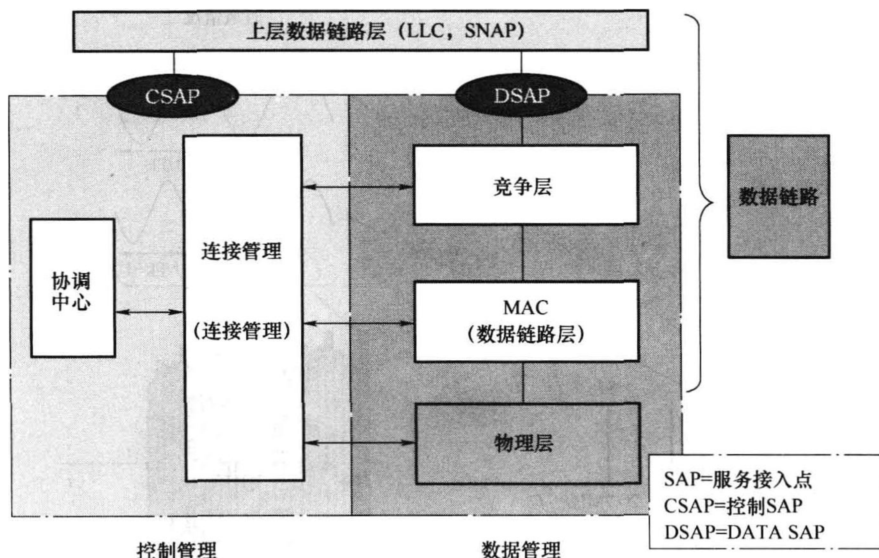


图 5.4　HomePlug AV 结构

这两个层同时管理两个功能，其中一个功能是网络的主从设备之间检查的管理，主要目的是提供不同的 QoS 功能；还有一个功能就是数据管理功能，也就是封装 MAC 的数据并保证上层数据可用。

5.2　OFDM 接口帧

OFDM（正交频分复用）接口是 PLC 应用的接入技术。ADSL、全球电视广播

技术，以及 IEEE 802.11a 和 IEEE 802.11g 标准的 Wi-Fi 也采用了这种接入技术。

这项技术就通信媒介而言具有很强的抗干扰性。OFDM 技术的原理就是把频段划分成窄的子带，每个子带用来传输二进制信息。每个子带的频率响应是正交的，并且混叠较小，这样就能够得到较好的频谱利用率。

5.2.1 OFDM 符号

如上所述，HomePlug1.0、Turbo 和 HomePlug AV 的帧结构中包含了合并成块的二进制 OFDM 符号。

图 5.5 示意性地给出了 PLC 技术所使用的 OFDM 频带的时域和频域示意图。频域上，频率被分成了 84 个子带。这 84 个子带仅使用其中的 78 个，以便满足相关频谱管理的规定，保护业余无线电业务（与 40m，20m 和 17m 的业余业务的频段相兼容）。

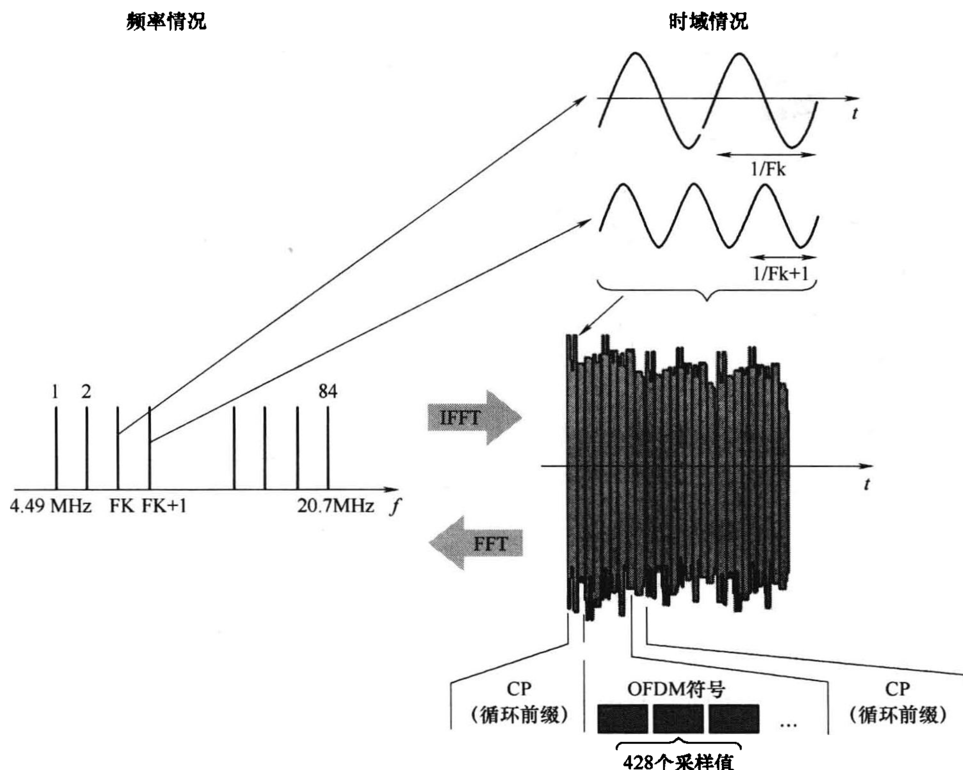


图 5.5 OFDM 频带时域和频域的示意图

每个承载 OFDM 帧的子带都由两部分组成：

1）循环前缀（Cyclic Prefix），用作传输数据部分的时间分割。

2）数据帧（包括 OFDM 符号），每个符号含有 428 个采样值。

HomePlug 帧的 OFDM 块包括 20 或者 24 个符号，ROBO 帧则包括 40 个符号。

图 5.6 给出了 OFDM 符号的细节和不同部分所代表的时长：HomePlug1.0 为 8.4μs，HomePlug AV 为 40.96μs。

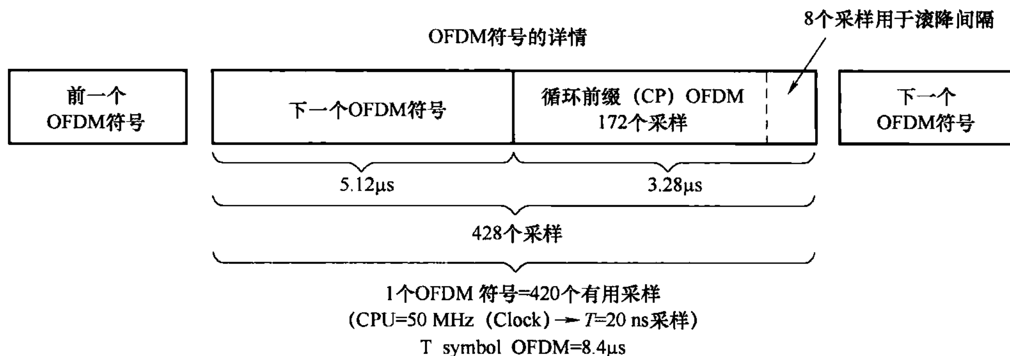


图 5.6　OFDM 符号的细节示意图

长数据帧本身包括 20 ~ 120 个 OFDM 块，形成了数据链路层和服务块的数据。

根据 PLC 设备之间链路的质量，OFDM 符号在每个频率子带上进行相应的相位调制。

OFDM 的传输机制

与单载波传输机制不同，OFDM 传输机制用来平衡发射机和接收机之间信号传输的功率均衡的复杂度，从而保证了 PLC 接收机的简单和经济。

OFDM 传输机制的其他优点如下：

1）与传统的频率复用技术不同，其频带利用率高。不同信道在频谱上交叠，但是保持完全正交性。

2）尽管降低了数据传输速率，由于保护间隔的存在，它具有数字均衡和简单理想的编码技术。综合使用卷积码、维特比码、块码（Reed-Solomon 码），这些技术可以提高效率。

3）由于使用多载波，它具有很好的抗脉冲噪声的性能。每个载波受到噪声干扰与其他载波相互独立。在单载波技术中，噪声影响多个符号，在 OFDM 技术中，符号仅在单一载波上损失，而其他载波不受影响。

4）每个用户或每个载波具有灵活分配的高比特率。根据物理链路质量和最适合的调制技术，可以对每个载波进行与其他载波相互独立的编码。

5）传输信道性能预估计的改善。在 OFDM 技术中，频域上使用了用来识别传输信道容量的学习帧（training frame）。

图 5.7 给出了 OFDM 符号在每个信道（频率子带）上的情况概览。

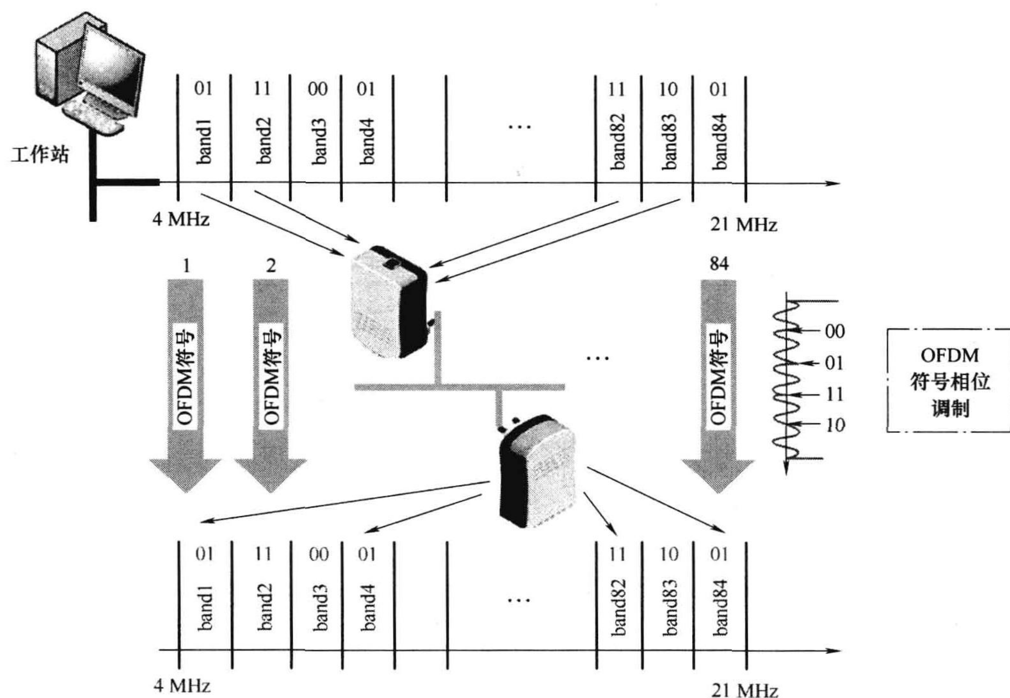


图 5.7　OFDM 符号在频域内的分配

HomePlug1.0 帧采用了数种调制、频率分割和纠错技术，这些技术构成了每个 PLC 设备在模拟的物理接口与 RJ-45 型以太网接口之间数据传输的方式。

5.2.2　HomePlug AV 设备的频带

充斥着较强干扰信号的媒介中的信号处理技术，为 PLC 工业企业带来了发展，使得它们能够最大限度地利用 1～30MHz 这个授权频段，并且实现约 200Mbit/s 传输速率的 PLC 解决方案。

在 HomePlug AV 之中，物理层上使用了 917 个频率子带。每个子带使用了 OFDM 符号，从而使其在频域按正交方式对数据编码。因此，这些子带从频率的角度相互独立而不会相互干扰。

在每个频带上，数据和它的 OFDM 符号用 Turbo 卷积码的方式进行编码。然后实现调制，自然每个频带都不同（见图 5.8）。

这种调制从 BPSK 到 1024-QAM 变化，BPSK 的每个符号和频带编码 1bit，1024-QAM 的每个符号和频带编码 10bit。

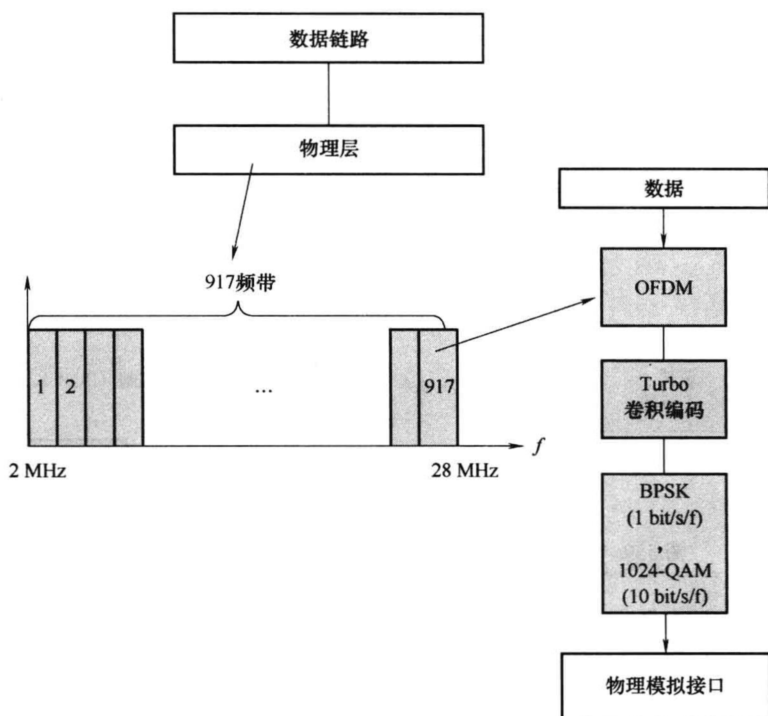


图 5.8　在 HomePlug AV 中频带使用的具体情况

5.2.3　功能模块

因此，一个 PLC 设备包含多种信号处理的电子单元[⊖]。在传输来自以太网接口或者从电力网接口数据的数据处理链中，这些电子单元扮演着某一特定的角色。

图 5.9 显示了用于不同网络 PLC 设备之间发送和接收 HomePlug 1.0 帧的功能模块。根据电力传输信道质量的不同，这些 PLC 设备都具有自动调节的功能。

自动调节的功能就是为了尽可能高效地使上层协议层和每个 PLC 设备以太网接口的不同终端获得理想的性能。

5.2.4　HomePlug 帧和 IEEE 802.11b 帧的区别

从功能性的角度来看，HomePlug 1.0 帧和 IEEE 802.11b 帧有一定的区别。

⊖ 这里所说的“电子单元”实际意为“组成部分”。——译者注

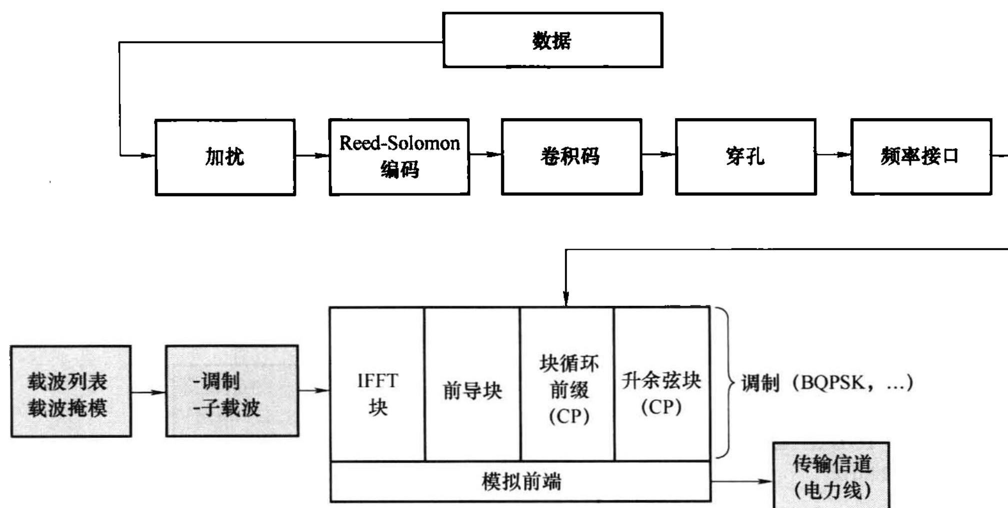


图 5.9　在 HomePlug1.0 中进行数据信号处理的功能模块

主要的区别集中在 PLC 技术的 MAC 封装这一环节。PLC 的 MAC 类型数据以完整帧的形式进行定义，然而 IEEE 802.11 帧还必须有 LLC 层以及一个更为复杂的 MAC 帧的重构过程。

图 5.10 用带箭头的方框给出了两种标准帧的不同之处。IEEE 802.11 标准在竞争技术和附加的帧间间隔等地方稍有不同。

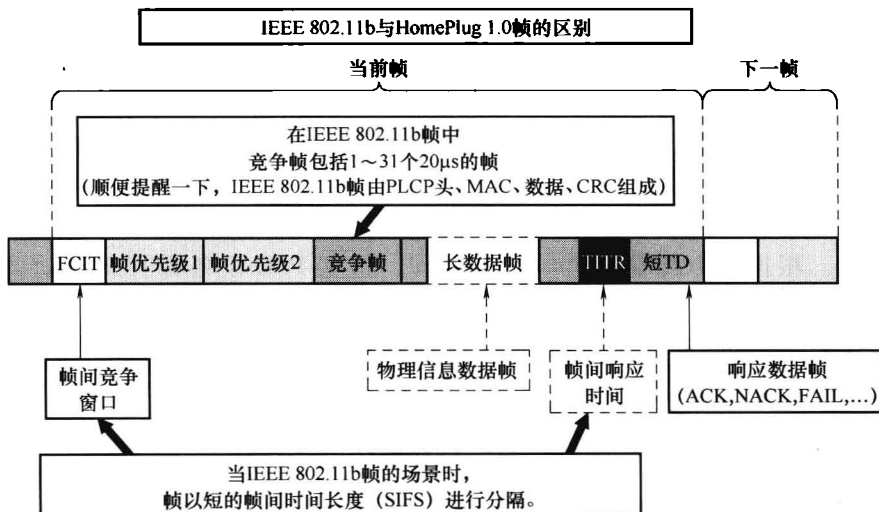


图 5.10　HomePlug1.0 帧和 IEEE 802.11b 帧的区别

5.2.5　PLC 物理帧

在 HomePlug 1.0 中，物理层帧，或者说物理 PPDU（物理协议数据单元）与 MAC 层的帧密切相关，这是因为 MAC 层的信息在物理层才变为可用。

物理层有两种类型的 PPDU，即长 PPDU 和短 PPDU。除此之外，物理层还有一些用于分隔这些 PPDU 或者确保 PPDU 有足够间隔的组成单元，这些单元确保工作站之间有足够的时间传输和接收帧。HomePlug 1.0 物理帧可由以下不同单元组成：

1）三个分隔符：

SOF（Start Of Frame，帧开始）：用来划定帧的开始之处；

EOF（End Of Frame，帧结束）：用来划定帧的结束之处；

短 PPDU：是目标工作站发回的响应，用来表示传输的数据已经收到。

2）在两帧传输之间的两个时间间隔：

CIFS（竞争分布式帧间间隔）：它在帧尾部，是帧结束分隔符之前的一个间隔；

RIFS（响应帧间间隔）：它是等待目标工作站响应时的一段时间间隔。

3）长 PPDU：它包含了数据帧。

图 5.11 给出了 HomePlug 1.0 和 Turbo 的 PLC 物理帧的所有组成部分，在图中，还有一个包含着上层数据的长帧，用于划分物理媒介中的帧边界的帧间间隔，以及用来管理 PLC 设备响应以及优化通信时间的短帧。

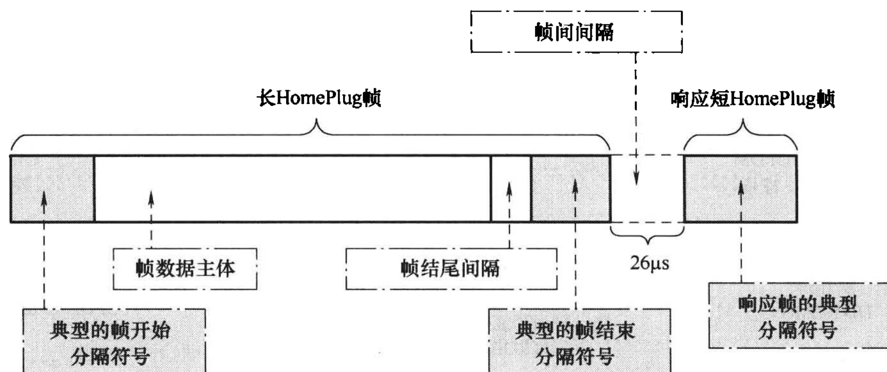


图 5.11　HomePlug1.0 物理帧的元素

物理层的长帧，被称作 PLCP PPDU（物理层通用协议 PPDU），也就是通过物理层发送的数据块。这些长帧，也被称作长的 PPDU，包括 6 个部分：前导、帧检验、帧头、帧主体、填充位以及 FCS。

1）位于 SOF 中的帧前导用来标注 MAC 帧的时间戳。

2）FC（帧检验）是用来检验帧的。帧中包含有 4 个 OFDM 符号，这些符号具有很强的抗传输信道噪声能力并且使用了 Turbo 卷积码。这种码被广泛用于 HomePlug AV 中的信号处理。这 4 个符号需通过传输信道进行传输，从而使接收端尽可能知道链路状态和传输数据的错误情况。

3）帧头包含了与传输速率相关的不同信息，这些信息根据信号质量而不断变化。

4）帧主体包含了来自 MAC 层的数据信息。这一信息也被称作 MPDU（MAC 层数据单元）。

5）当有用数据达不到最小帧的大小时，填充位用来填充这个帧。

6）FCS（帧检验序列）用来检验帧主体中的数据的完整性。

当没有优先级和竞争帧头时，所有 HomePlug 1.0 帧的长度大约为 1.5ms，包含由 160 个持续时间为 1.328ms 的 OFDM 符号的帧主体。

图 5.12 给出了 HomePlug 1.0 和 Turbo 中长帧的各个要素。这种长帧通常包括 3 部分：帧的开始，其被用来识别网络中的长帧；数据（包含上层数据帧主体）；帧的结束，用来识别帧的结束，从而告知 PLC 设备可以发送下一帧。

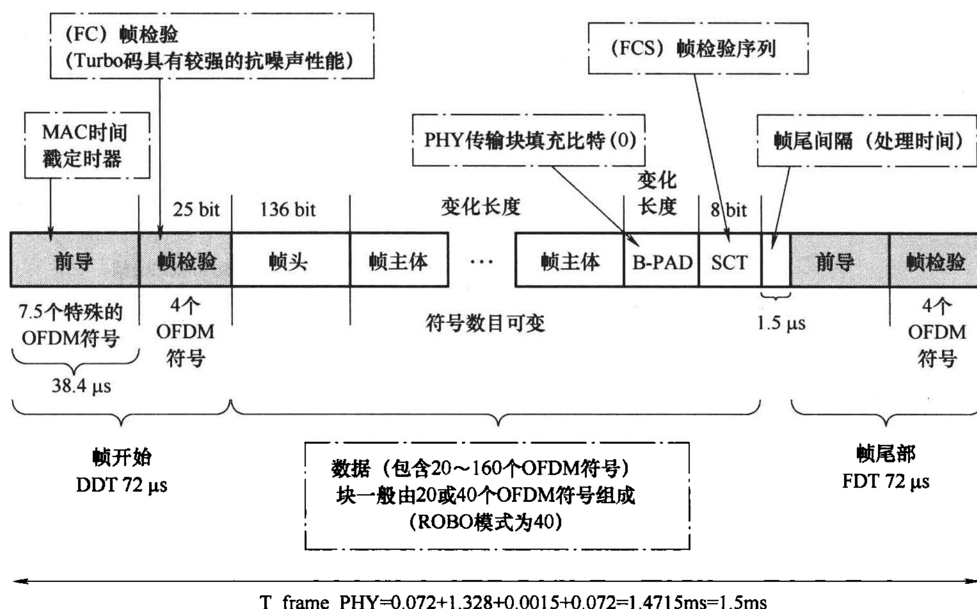


图 5.12 HomePlug1.0 的长帧结构

物理帧的开始分隔符

开始分隔符包括两部分，即前导和 FC（帧检验）：

1）前导包括了帧的发送时间戳。

2）FC（帧检验）包括几个部分：竞争检验部分，用来检验传输帧的竞争程度；记载分隔符的类型部分；可变的部分，这一部分包括两个特别重要的关于PLC通信的内容（载波列表，它存储了PLC设备之间的链路状态；下一帧大小信息）和帧检验序列部分。在最后一部分中使用了CRC（循环冗余校验），用来检验帧的完整性（见图5.13）。

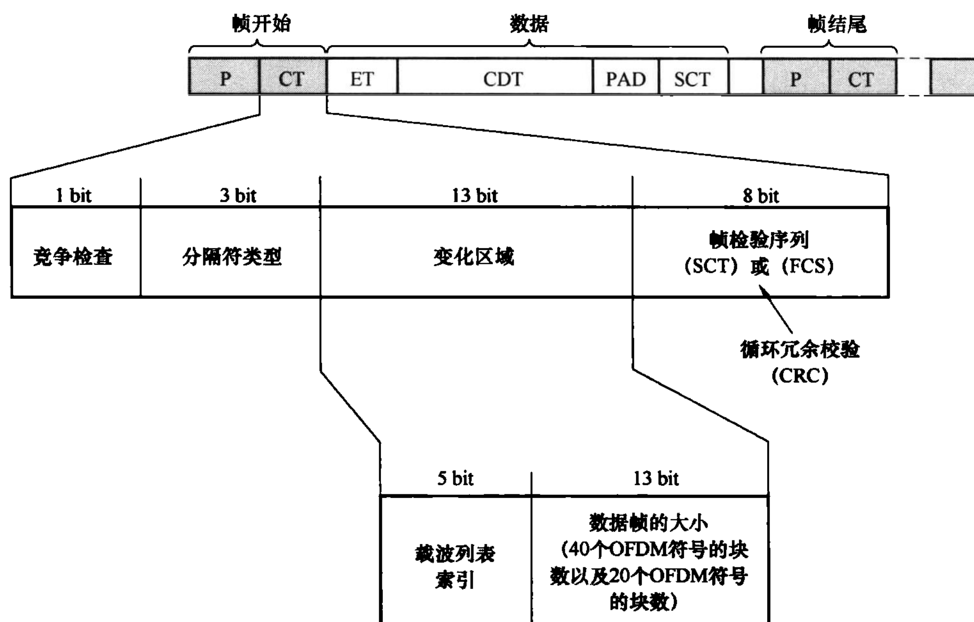


图5.13 物理帧

物理的数据主体

物理帧的数据主体情况如图5.14所示。它包括封装在PPDU中的MDPU。这种MPDU包括EB（数据块首）、PAD（填充位）（当数据不能完全填充数据部分时）和SCB（比特检验序列）三部分。SCB用ICV（完整性检验值）来检验数据主体的完整性。

物理帧的结束分隔符

物理帧以结束分隔符结束，其包括前导和帧检验部分。

帧检验部分包括4个部分（见图5.15）：

1）竞争校验，用来检验帧间竞争的时长状态。

2）分隔符号类型，指定分隔符是在帧头还是在帧尾。

3）与这个分隔符相关的特定变量，其包括PLC站的优先级状态（用CAP参

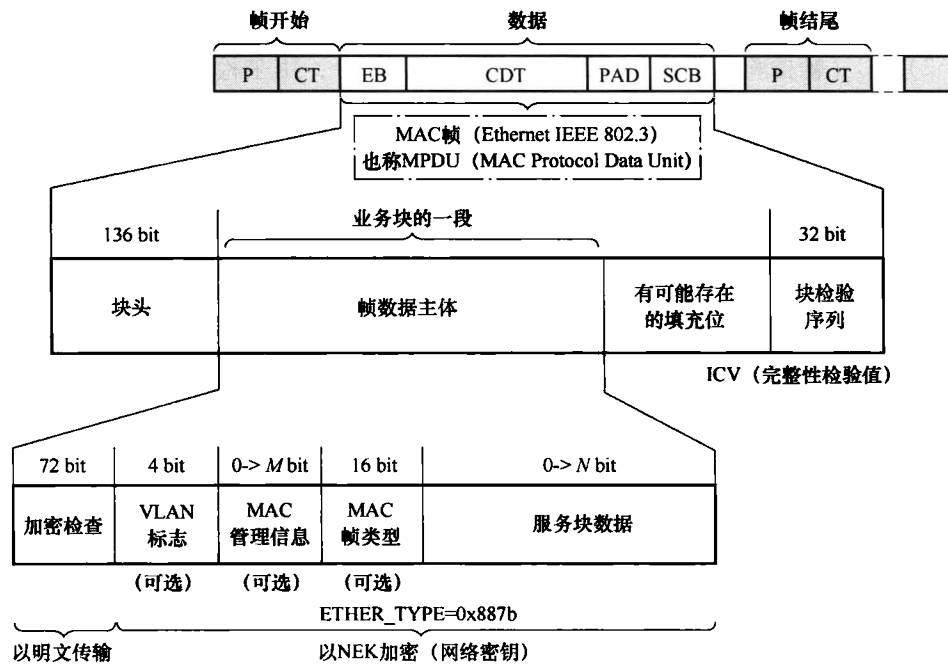


图 5.14 物理帧数据结构

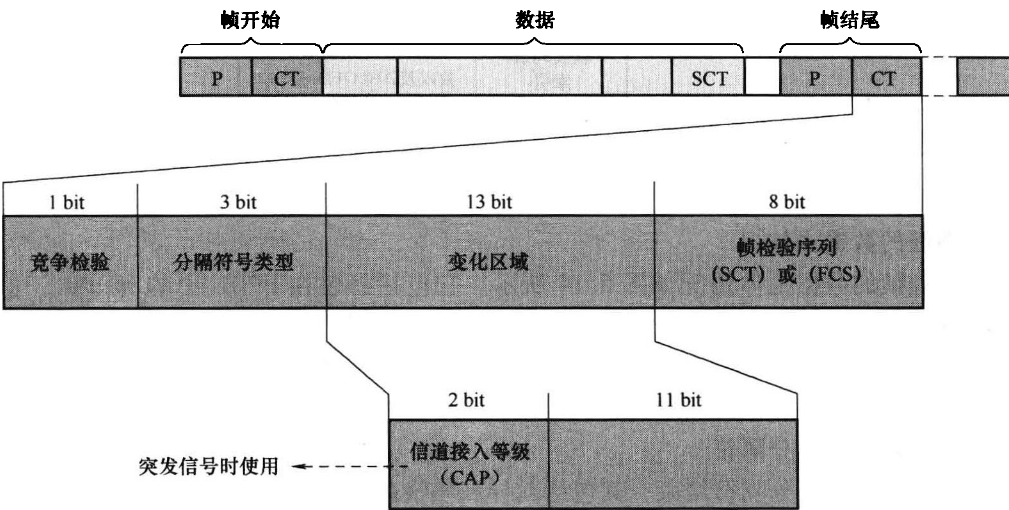


图 5.15 物理帧的尾部结构

数表明）。

4）FCS，它使用了 16bit 的 CRC，用于确认帧的完整性。FCS 在帧的帧头和帧

主体中都有。FCS中使用的技术在链路上的帧传输主流标准中很常见。

5.3 MAC层帧

MAC（媒体接入控制）层帧，位于物理层的上方，并且有一条链路通向上层。

正如前文所述，PLC技术被看作是一个MAC层的封装技术，因为MPDU帧被封装在长PPDUs中。同样，所有源于MAC层之上的数据都被封装于MAC帧之中。

5.3.1 MAC HomePlug 1.0 帧

HomePlug 1.0中，封装好的IEEE802.3或MPDU（MAC协议数据单元）帧位于PLC帧的帧主体之中，并且位于起始和结束分隔符之间。

在以太网中，以太网HomePlug 1.0帧容易被识别，因为对于所有帧，十六进制的0x887b值被记录在MAC ETHERTYPE的帧类型域中。使用这个参数专门为PLC技术在数据链路层中创造各类应用。在HomePlug AV情况下，ETHERTYPE域的值为0x88e1。

除了72bit的加密检验之外，帧的数据主体用网络中不同PLC站间交换的NEK（网络密钥）进行加密。

MPDU构成了服务块（BS）。如果BS超过了MAC帧的限制值（1500B），BS被发送工作站分割成几个序列发往接收工作站。

MPDU分割成的每一个部分都被编号，并且可被接收工作站按照顺序重新组合起来。

5.3.2 MAC帧头格式

MAC帧以一个非常复杂的帧头开始，它包括3个部分，总长为17B（见图5.16）。

块检验部分

帧头的第一部分包括40bit，并且它被分割成8个子部分。这部分的目的是为了传输MAC层需要的检验信息。

图5.16给出了帧检验部分及其子部分的情况。不同子部分的用途如下：

1）协议版本。定义了所使用协议。这个数值是保留字，只在标准演进的时候使用。

2）桥接。它表明这个PLC工作站传输数据是否处于桥接状态，它还可以为那些发往其他网络工作站的帧起到接力的功用。

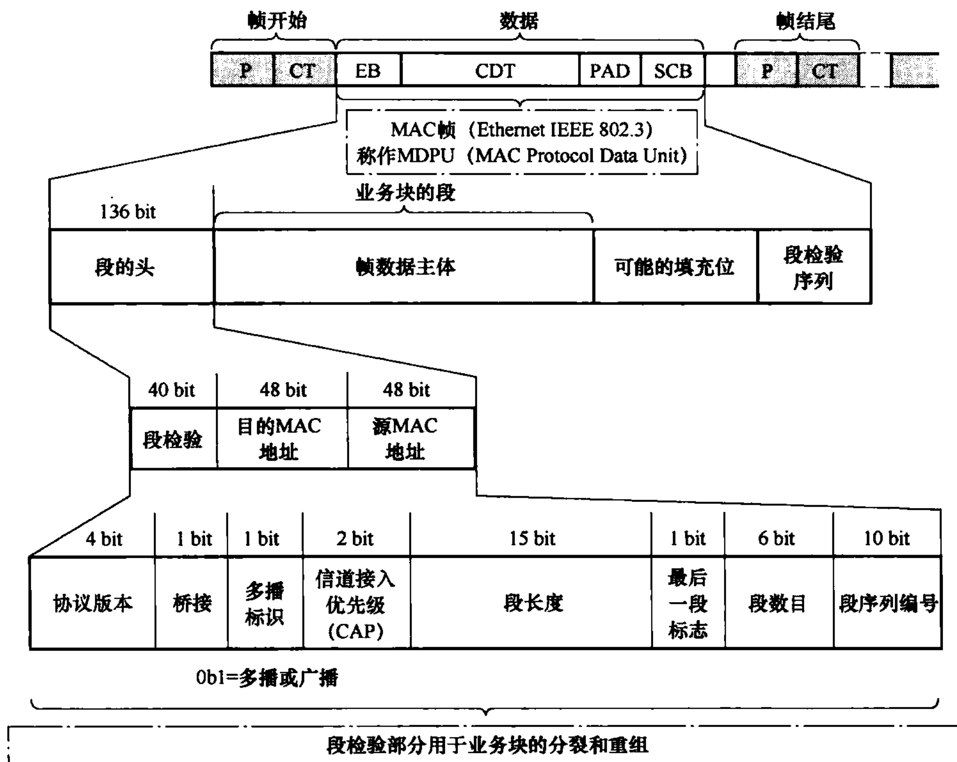


图 5.16 HomePlug1.0 的 MAC 帧头

3）MCF（多播标识）。它表明这个帧是否以多播的模式发送，如果这个数值为 0b1，则帧的发送为广播模式。

4）CAP（信道接入优先级）。和 PLC 网络其他站点相比，发送工作站优先级的复用。

5）段长度。用来给出传输段的数据长度。

6）LSF（末段标识）。如果值被设为 0b1，这个段就是最后一个段。

7）段数目。记载了不同的 BS 段分割和重组的顺序。

8）段序列编号。这个编号默认值为 0，并且被分配给每个帧。对于所有已经传输的帧，这个数值以 1 为步进增加。如果帧被分割，则这个帧的所有段都有相同的序列号。

地址域

在 HomePlug 中，所有地址域有 6B 长，和 IEEE 802.3 标准中定义的地址相同。48bit 地址包括以下 4 个部分：

1）个人/组（I/G），首个 bit 表示地址是个人地址（1）还是组地址（0）。

2）通用/本地的（U/L），第二个 bit 表示地址为本地地址（1）还是通用地址（0）。如果是本地地址，那么接下来 46bit 也被定为本地的。

3）统一组织的识别器。在 I/G 和 U/L bit 后面，与 IEEE 分配的 22bit 数一样。

4）序列号。最后 3B，即 24bit，通常是由厂家定义的序列号。

十六进制格式

通常 MAC 地址用十六进制表示，比二进制更好。

MAC 地址由两个不同的地址组成：个人地址，赋予网络中单个站的地址；以及组地址，指配给网络中多个站的地址。在后面情况中，MAC 地址代表一组地址。

有两种形式的组地址：

1）广播地址：这是一种网络中的工作站都包含的组地址。使用广播地址可以将信息发送到所有网络中的工作站。广播地址总是 48bit 的格式。所有 bit 被设为 1。

2）多播地址：与广播地址相似，这一地址为一群工作站所共有，只不过数量上更为有限。这种地址的首 24bit（48bit MAC 地址中的首 24bit）均为 01：00：5E（十六进制）。

类似地，HomePlug 中 IEEE 802. 3MAC 帧包括如下两个地址域：

1）DA（目标地址）。帧或段传输的目的地。DA 地址可以是个人地址也可以是组地址。

2）SA（源地址）。传输过来的帧或段的源地址。SA 地址总是个人地址。

5.3.3 加密的 MAC 帧的格式

IEEE802. 3 标准使得帧可以通过电力线媒质加密，从而保证非法用户无法破解信息。

在实际中，如图 5. 17 所示，一个帧一般仅仅部分加密。帧采用如下两种方式进行加密：

1）IV（初始化矢量）。具有大量 bit 的初始化矢量与一批用于解密帧的重要数据相连接，每次使用后被重新初始化。IV 和数据的结合产生了独一无二的密钥。

2）EKS（密钥选择）。用来恢复信息以便解密帧内容。

5.3.4 控制和管理帧格式

控制和管理帧的目的是向那些网络单元发送监管信息和命令，使它们工作。

如图 5. 18 所示，源工作站需要关于帧长和帧响应的信息，从而管理和控制帧（参见第 3 章）。

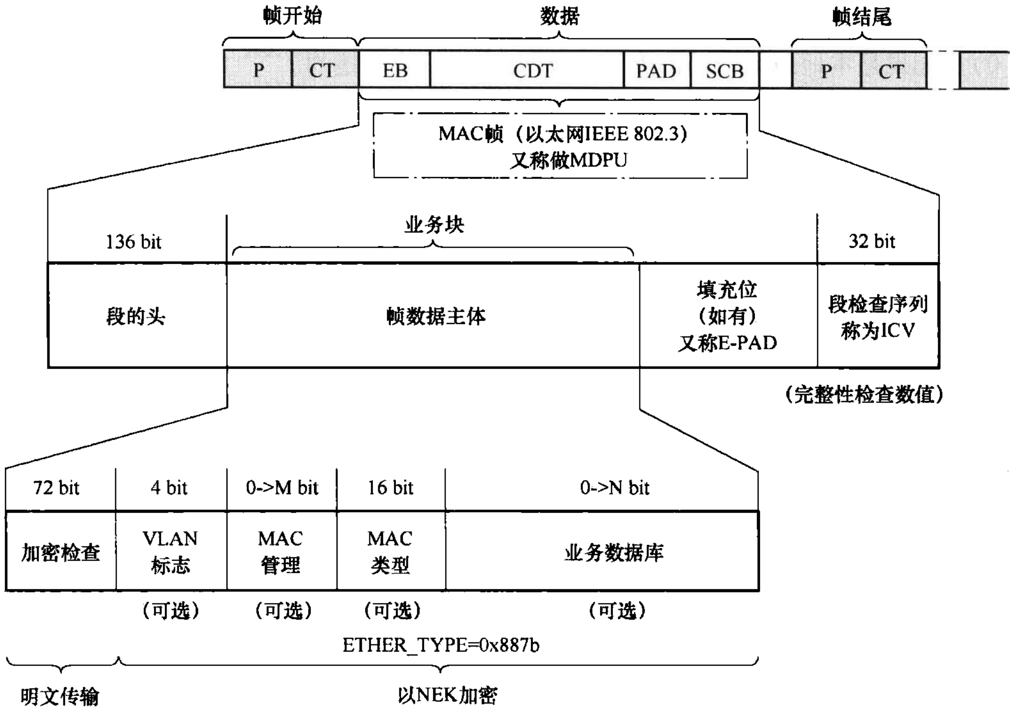


图 5.17　被加密的 HomePlug1.0 的 MAC 帧

一些生产商的 PLC 产品设计了特殊的 MAC 层，因此管理和控制网络更加简单。

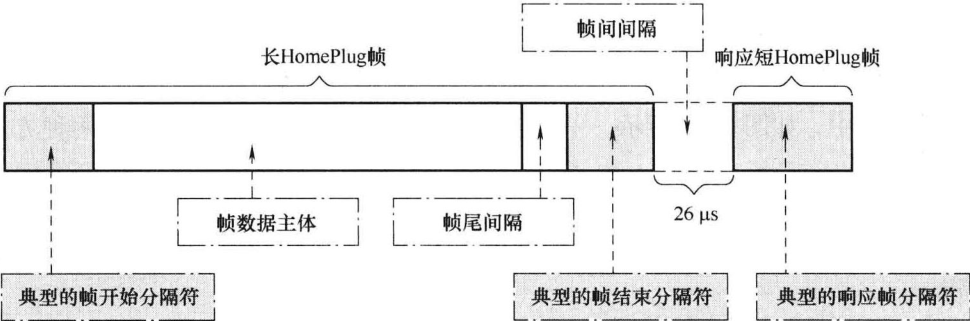


图 5.18　PLC 帧的控制管理域

第 2 部分

PLC的实际应用

本书的第 1 部分介绍了 PLC 网络的结构，从理论的角度解释了它们如何运行。本书的第 2 部分将着眼于实际应用，详细叙述安装这种网络时所需遵循的规则，重点在于这种新应用基于电力网实现数据广播的概念，以及在电力网上的制约、选择、安装和设备配置。

PLC 网络的简化和实用性意味着它能够快速发展，并且能够适应 PLC 技术的新版本，开拓新的应用。在不久的将来，适应 PLC 的 IEEE1901 标准也将出台。

从应用的观点看，PLC 网络不会带来巨大的技术变革，而是应用在一些普通的场景之中，例如音频和视频等。不过，使用电力网络传输高速率数据会带来意想不到的应用，如在机动车上传输数据或者用 PLC 作为 Wi-Fi 网络的骨干网。

我们仍然处于这些新技术的早期阶段。毫无疑问，随着时间的推移，这些技术应用将向用户友好、简化方向演进，并将综合更多特殊功能，逐渐引起用户的关注。

虽然 PLC 的原理粗看上去比较简单，但如果关注到它的细节，情况就有所不同了。在电学方面，关注电力网络拓扑结构和接口在安装 PLC 网络时是很重要的。另外，区分可用吞吐量和理论速率的概念也是非常重要的。这种速率与网络传输速率有关。由于不同层的网络协议所应用机制的不同导致了可用速率相对较低（物理、数据链路、网络、传输等）。这些机制在第 3 章和第 5 章已经细致讨论了。

在过去的数年，PLC 网络的基础设备高速演进。最初，以笨重的台式机产品形式出现的终端不能满足用户的需求。现在，设备有各种多个接口和许多完整的网络功能（路由器、调制解调器、Wi-Fi 接入点和交换机等），并且用户已经习惯的传统配置方式也可以使用。

配置 Wi-Fi 网络是从配置终端和相应的 PLC 适配器开始的。本部分将详细叙述在 Windows XP、Linux、FreeBSD 操作系统中如何进行配置，一旦终端被配置，就会启动安装。在此阶段，还需要考虑电力网络拓扑结构、安全性和性能等方面的约束。

本部分的各章将逐步介绍需要注意的事项以及配置的步骤，读者在阅读完本部分的各章内容后，可以在不需要协助的情况下最恰当地安装和配置网络。

介绍完本部分之后，本书的内容也就全部介绍完了。在本书的最后，我们将介绍 PLC 网络未来的标准化趋势。我们相信在不久的将来，PLC 网络将会成为家庭环境和专业环境下的一个基础的网络组成部分，并将进一步提升家居自动化水平。这里所说的家居自动化水平是基于在房间或者建筑物内的数据交换。

第6章　应　　用

一些前瞻性研究显示，数年后，90%的网络终端将不是计算机。这一前景还表明，一些领域（如工业、医院、家庭自动化、电子、数字艺术等）的任何类型的电气和电子设备，将配备RJ-45网络接口来连接本地以太网。

可以看到，最近一些年网络上已有的两个主要标准——以太网和IP的优势。从这些情况来看，我们可以有理由认为设备之间的通信网络将主要通过最方便、最可靠的通信介质来解决。从这一点来看，PLC无疑将成为拓展电力网络（插座网络和光网络等）应用的主角，赋予不同的设备各式各样的最新的网络通信的功能。

在网络世界，PLC网络带来了一些新的亮点。最主要的亮点莫过于操作的便捷性。因为用户通过建筑物的插座就可以建立一个计算机网络。

安装好网络之后，就可以为实时的多媒体应用提供足够的数据传输速率。除此之外，它能作为Wi-Fi网络的骨干。PLC网络可以很好地完善Wi-Fi，使它能扩大其覆盖范围并且为其提供更好的技术支持。

6.1　声音、视频和多媒体

声音和视频是实时应用，在异步传输网络（比如PLC）中是不容易实现的。然而，作为电话应用网络的拓展，它们可能成为这些网络未来的组成部分。

传统电话是围绕PABX分布的，不过从2005年开始，PABX连接到电话机的配电线路开始被PLC环境下的IP电话（Telephony over IP）取代。现在，自从2007年初，PLC网络已经成为广播电视传输信道，并且还能够在用户间实现视频会议。作为多媒体应用，PLC迅速成为相当数量公司的选择。

6.1.1　PLC电话

传输速率不是传输电话语音时的主要问题，因为速率低到5.6kbit/s都可以，PLC网络支持这一速率还是绰绰有余的。

另一方面，因为电话应用是互动的，在信息由一个使用者发送，接收者接收的时候延迟一定不能超过300ms。如果它是一个对称网络，来回的最大时间一定不能超过300ms，因为这是人们可接受的最大时延数值。

当传输电话语音的时候，同步是第二个制约。信息必须在精确的时间内准确、有效地送达接收者。特别是源于数字化采样的字节必须在完全确定的同步时间内传

送。例如，如果压缩生成了一个 8kbit/s 的流，这涉及每微秒同步。因此，1B 的数据必须在 1μs 传送到接收者。如果语音没有压缩，一个 64kbit/s 的信道每 125μs 同步一次。

PLC 电话的第三个主要特征是 VoIP（基于 IP 的语音通信）技术的使用。语音字节在 IP 数据包中传递，并与传送其他应用程序的数据包同时使用网络资源。因此，基于 PLC 的电话通过 IP 融入了传统的 IP 语音（Speech over IP）的框架。

图 6.1 说明了远程电话方面的同步制约。尽管发送者有规律地发送数据包，但是它们是在不等的间隔内接收的。因此，想在精确时间传递语音字节，对于接收者是十分困难的。因为通过了 PLC 网络传输所以数据接收就没有规律，语音数据包将随机抵达。

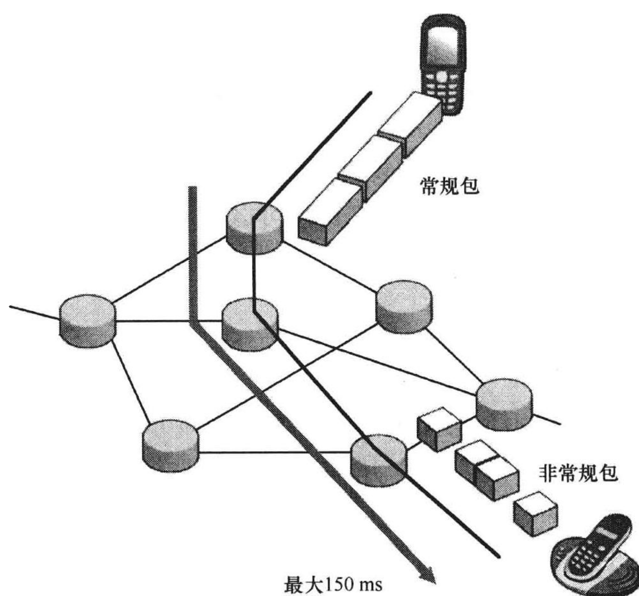


图 6.1　电话通信制约

接入方法是用来获得权限，从而将数据传送到接入点，CSMA/CA（载波侦听多路访问/冲突避免）机制随机使用 PLC 网络。除此之外，为了到达接收端，数据包必须通过更广泛的网络，并且随机通过中间传输节点。

语音打包和解包

假设语音被压缩成 8kbit/s，这是基于 IP 环境的最通常的语音标准。

电话字节必须被打包成为 IP 包，为了在电力网络中传输，这个 IP 包封装至一个以太网帧，准确地讲，是将其封装如一个 PLC 帧，以便在电力网络上传输。

对于8kbit/s的速度，每1ms同步一次。如果N代表能在PLC中使用的字节数，那么整个打包时长[⊖]为N个1ms。因为PLC帧的最小长度是64B，因此打包需要64ms。

解包工作是在打包工作进行的同时开展的，所以实际上并不需要额外的时间。这样一来，打包—解包需要的时间至少为64ms。事实上，现在的趋势是考虑打包—解包等待时间这一因素，增加对打包和解包耗时的预估。

64ms时间在150ms出口路径情况下是可接受的。然而，如果封包必须通过网络而不是PLC网络，或者如果打包—解包太慢，64ms这一数值就显得太高了。这就是为什么语音包仅为16B，且剩余的部分字节通过填充字节达到最小帧尺寸。对这16B的打包—解包时间大约仍保持在16ms。

实际速率

事实上，网络中的实际速率远远高于8kbit/s，因为数据封包有包头和填充字节之类的附加信息。我们认为使用IPv4标准并被封装成以太网帧，一个基于PLC网络或者其他封包传递网络的实际数据速度大约是60~70kbit/s。

如果使用IPv6标准，管理领域甚至更大，这时一个语音信道将会超过100kbit/s。

编码—解码器（简称编解码器）对模拟信号数字化的时间以及数字信号模拟化的时间大约为5ms。因此，编码、解码和打包—解包共需要26ms。总的可用传输时长将变成124ms（正如本节开始介绍的，最大传送时间是150ms，减去26ms各种各样的时间）。这个传输时长包含了MAC接入到PLC网络的部分。

转接时间

在PLC中，接入电力线介质所需要的等待时间可能会比较长。例如，如果5个客户通过使用1500B帧连接到相同的电力网络，并且整合有关的CSMA/CA接入时间，等待时间大约为10ms甚至更多。如果假定电话的接听者是连接到PLC网络的同一公司的另一位雇员，那么接入网络的时间还需要再增加大约10ms。

假定话务量高但是没有发生碰撞，那么总的转接时间仍然大约为100ms。这个转接时间使得在PLC网络上传输电话语音成为可能。

随着HomePlug AV标准及其竞争者的发展（由于当前这一代PLC不能管理优先级），其他用户的数据封包也有着同样的优先级，即便它们传送的数据不是最急需的。例如，一个客户工作在一个点对点（P2P）的应用上，并且正在续传一个几个GB的视频文件的数据封包可以在一个电话用户数据封包之前传播。这是为什么对当前的PLC技术需要采取强力措施制约用户数量或者空着总的话务量。下一代

⊖ 8kbit/s相当于1kB/s或1B/ms，若每毫秒同步一次，那么打包N B需要耗N ms。——译者注

HomePlug AV 的 PLC 将有能力管理电话和视频包的优先级，以确保基于该数据网络上的业务质量。

如果用户数量超过 10，或者有用传输速率超过 5Mbit/s，此时则不能保证利用 HomePlug 1.0 PLC 网络传输电话语音的可靠性，也就是达不到必要的服务质量（QoS）。在这种情况下，必须使用另一个技术对电话语音包指定优先权。

区分 IP 包

就目前来说，可以采用两种解决方案来区分 PLC 上通过的封包。

1）IP 协议层的 IP 包控制技术。在这种情况下，PLC 网络管理者（管理单元）在接收工作站，暂缓那些不具备优先级的封包的确认信息的传入，这样一来这些数据流将维持在一个低星级的状态，发送者只能发送少数几个封包，且必须等待进一步的传输确认。

2）使用 HomePlug AV 标准，该标准在 2007 年发布。这个标准在 MAC 层决定优先级。在这种情况下，给电话业务指派最高优先级是足够的。

第二种解决方案显然是最好的，因为它能应用在结构的最底层并且明显地有利于电话语音流。另一种解决方案更加智能一些，因为它包含优先级控制，不用去顾及具备优先级的语音客户的实际带宽要求。

图 6.2 示意性地给出了除了从一个终端到另一个终端的语音通信之外的 PLC 网络应用（及其相应组件），这些应用都在同样一个 PLC 网络中。

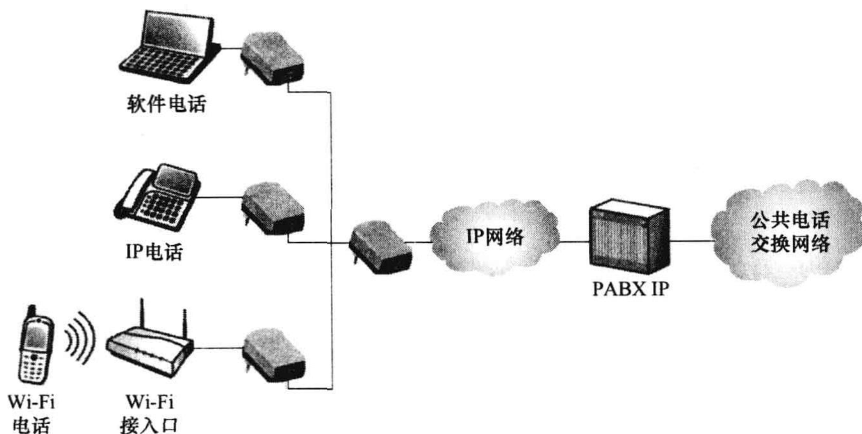


图 6.2 通过 PLC 数字语音流连接的设备

在通过输出 PLC 网络后，语音数据流在一个固定 IP 网络中传输，这个网络可能是一个运营商网络。然后，在进入传统的电话设施之前，通过一个专用网关（PABX IP）。这个网关把 IP 地址转换成电话地址，并且执行必要编码转换工作，

转换成一个64kbit/s压缩数据的语音数据流。

Asterisk软件常用于创建一个IPBX（PABX），由它在服务层管理本地IP呼叫和流向STN（电话交换网）的呼叫。

高保真电话

PLC用来传送比传统电话语音更高质量的语音。事实上，因为PLC在传输速率上没有制约，所以提供较大的带宽从而传输高保真（Hi-Fi）语音或者近似高保真的语音。

假定你将512kbit/s的语音压缩成64kbit/s。传输64B的语音数据，只需要8ms。一般地，IP封包流的传输速率和以前相同，但是这个封包没有填充（padding）字节，也就是说它仅仅包含有用字节。因此，以同样的实际传输速率就可以传输更高质量的语音。

不过，这一技术的应用并不广泛，其原因是电话机并不都兼容高保真语音信息。这一兼容性能通过使用一个有声卡的微机解决。不幸的是，这个解决方案被证明是不完善的，因为市场上的声卡速度非常慢并且要求大约50ms的处理时间。当不得不使用两个装置（发送者和接收者）时，传输时间是不可接受的。

无论如何，这一实例表明基于PLC的IP语音业务是具有更高质量的。

视频

视频是PLC网络的另一个应用，并且它在未来会大放异彩。这一应用特别需要在一个高传输速率的PLC环境下实现接入。

目前，（视频传输）时间上的制约或多或少都是存在的，这一问题是视频应用需要考虑的。下面主要研究两个场景，视频流和视频会议。

视频流

对于没有回传信道的视频流（譬如视频点播即VoD和电视），视频流从节目源发送到该视频显示在屏幕上需要耗费相当长的时间，这个时间长度大约为秒级，甚至达到15s。在观看者看到图像之前，他（她）没有必要关心视频源是否正常工作。

这些应用最主要的制约就是在视频开始前的等待时间。就算是在接收端重新进行同步，等待应用程序自我初始化的耗时也令人十分反感。数据流之所以在展示给用户之前停顿一下，是为了让接收机的内存中缓存足够的数据封包，以防用户在使用数据包时产生中断。图6.3说明了这种制约。

视频可为数字化的模拟信号（被压缩）或者来自经压缩的数字信号。这些信号被大大压缩，且需要更高的传输速率。传输速率的具体数值取决于网络的能力以及发送端和接收端的计算能力。

传输速率越高并且压缩率越小，图像质量就越好。在传送视频图像中，对传输

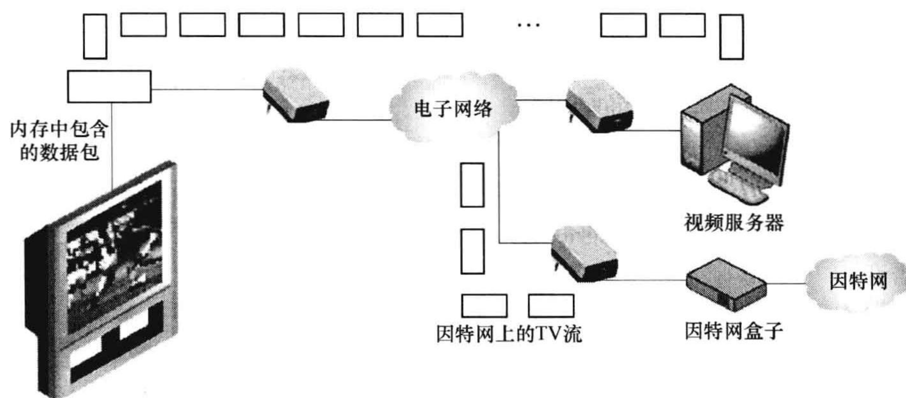


图 6.3　PLC 网络上的视频应用

速率的要求是一个重要因素。只要网络不饱和，这个因素不是 PLC 网络的主要问题。让我们首先分析传输一个视频信道的必要传输速率。

传送视频的必要的传输速率

视频设备主要使用最新的 MPEG 标准，DVB（数字视频广播）也已经被广泛应用。

MPEG 使用了帧内和帧间压缩算法。其传输速率可以降至 1.5Mbit/s，并且与原始图像相比，压缩质量损失很小。采用大约 4Mbit/s 传输速率的 MPEG-2 技术改善了图像质量。条件允许的话，可以考虑采用 MPEG-4 标准，应用更高的压缩比，并且增加用于在另一端重现图像的必要的某些元素。

广播电视传播的难点在于其传输速率并不固定，并且必须进行自行调整以适应传输网络。根据时间和介质中可用的资源，算法或多或少要压缩信息。如果网络几乎完全可用，图像质量能够提高不少。反之，若网络被来自于不同数据源的其他混合信息所充斥，就必须考虑降低视频传输的等级，当然这必须满足用户端的 QoS 需求。为了充分优化该应用传输，必须有一个控制机制。

为了满足使用者的节目质量的需求，高清数字电视（HDDTV）大约需要 5 ~ 10Mbit/s 的传输速率。5Mbit/s 传输速率太大了，对 HomePlug 1.0 和 Turbo 网络而言，支持这样的速率存在困难。如果使用 HomePlug AV（40Mbit/s），同时只能有两个用户能使用这项服务。

虽然 HDDTV 可以在 PLC 网络上传输，但是最大用户数量不能超过 10 个。

传输负荷（能力）问题

PLC 网络必须有能力提供连接，使视频应用使用最优传输速率，这个传输速率能确保一个可接受的服务质量。

我们首先看一下负荷量问题带来的困难。对电话语音没有问题，是语音因

为一旦被压缩，其数据流的传输速率是8kbit/s，甚至是5.6kbit/s。与此相对，对一个 MPEG-2 电视质量图像而言，负荷量要求在 2～8Mbit/s 之间。对 MPEG-4，这一要求下降到1Mbit/s。也就是说，不管怎么样，当前对能力的要求都在2Mbit/s左右。如果通过降低视频的质量，那么这个值有望下降至几百kbit/s。

对视频的播放质量，如果 HomePlug 1.0 网络的传输速率不足，那么 HomePlug Turbo 网络或者 HomePlug AV 网络的传输速率应该满足。因为对后两种网络而言，其提供的有用传输速率大约是10Mbit/s 和40Mbit/s，这一数值已经粗略地估计了自己的数据流和其他应网络应用的数据流。

与语音传输类似，可以采用优先级分类技术，给数据流的传输定义较高的优先级。在这种情况下，通过使用 HomePlug Turbo 和 AV 网络就不会在有传输速率的问题。

如果网络负荷容量充足，且用户的数目远远小于所需的负荷量，或者实施优先级分类，那么要解决第二个问题就是关注对字节再同步导致的延迟的处理。这就是为什么延时大约是几秒，甚至是几十秒也是必要的。这种情况下，一旦视频流的开始使用时，最初的图像只有在这个延迟之后才出现。

6.1.2 图像会议与视频会议

图像会议和视频会议应用于人际互动，并要求有150ms 的时延。正如前面所介绍的，必须研究数据再同步过程，以便将应用数据重组并同步到接收机。基于这个目的，服务质量（QoS）就与应用数据的传输息息相关了。

这两种应用类型的不同，源自于广播图像质量的不同。

在图像会议中，由于每秒的图像数量比正常水平低，因此图像可以是黑白色以及忽动忽停的。这些应用可以使用较低分辨率的屏幕从而降低传输速率。这也就需要网络的传输能力不超过100kbit/s。

视频会议要求较高的传输速率（若干个 Mbit/s），来获得比电视传输所获得的质量好的图像。为了达到影院级别的质量，必须达到大约50Mbit/s 的传输速率。需要考虑到的是，在现有的 HomePlug1.0 网络框架下难以达到这一速率，但是也许可以在 HomePlug AV 这代网络框架下得以实现。

这两种应用的难点主要是控制图像的即时再现。这两种采取的语音技术可以在 IP 层或者 HomePlug 帧层实现同步优先级管理。后者能够给 MAC 层的随机接入分配优先级，并且极大地减少具有优先级的工作站的等待时间。换句话说，具有优先级的工作站只要有数据帧需要传输，它就比其他工作站优先传输。唯一的条件就是优先站的总传输速率始终要比获得的网络有用吞吐量的值要低。

在 HomePlug1.0 PLC 网络中，广播高质量视频会议是不容易的。当 HomePlug AV 的传输速率达到 200Mbit/s 时，如果客户端的数量减少一些，传输一个或两个高质量的视频会议信道是可能的，尽管失去同步的概率会随着流量的增加而快速增加。

6.1.3　多媒体

多媒体一般地都会将至少一种语音或视频流重叠到其他数据流上。与语音或视频相比，这种多媒体应用不会对 PLC 网络造成更大的问题。唯一增加的制约就是为了实现多媒体进程而带来的实时应用的同步问题。

网络在传输多媒体应用时，必须在复杂度和传输时间之间达到一个折中。为了再次找回数字文件的原始信号质量，我们考虑压缩必须控制在 3 级。在图像应用中，图像的质量非常重要，就像 X 射线影像学那样。固定图像的压缩因子在 10～50 范围变化，而在视频中变化范围达到了 50～200。对固定的图像平均压缩因子是 20，而视频的平均压缩因子则是 100。

这些压缩造成了图像的微小失真，并且可与用人眼的恢复能力补偿。这是因为人的眼睛对亮度更加敏感，例如对图像亮度要比色度和颜色敏感。这个特性在高清晰电视的编码中再次得以印证。电视的亮度分辨率是基于 720×480 个点的图像，而此时的所用色度却是 360×240。亮度每个点所要求的编码都比色度要多。

我们已经了解了 PLC 网络能支持必要的码速率来传输多媒体应用的数据流。为此，接入电力网络的客户端数量需要限制（参见第 3 章）。

因此，在 PLC 在网络负荷容量（能力）方面的问题要比在时间管理方面要少一些。在异步的网络中（如 PLC 网络），实时性和同步性这两方面的制约很难突破，因为在这些网络中没有时间管理器，并且数据传输也不是采用确定的方式（参见第 3 章）。

服务质量（QoS）

正如第 3 章所介绍的那样，HomePlug1.0 和 Turbo 技术中没有服务质量（QoS），因为数据传输时间不是确定的。服务质量必须在 MAC 层之上的应用层来实现，以此来补偿这一不确定性。

HomePlug AV 中实现了对服务质量的要求。HomePlug AV 能向不同的业务提供所需的传输速率和稳定的传输时间。每种数据业务的 TDMA 时隙实际上就分配了服务质量。

表 6.1 给出了不同应用场景下的不同 PLC 网络的用户情况（一对夫妇，一对有三个小孩的夫妇，一对有一个小孩和两个十几岁孩子的夫妇）。

表6.1 PLC网络的应用场景以及对应的用户情况

应 用	必要传输速率	应用场景					
		一对夫妇		一对夫妇+三个小孩		一对夫妇+一个小孩+两个少年	
		数量	传输速率	数量	传输速率	数量	传输速率
家庭影院 HDTV	22~28Mbit/s	1	22~28	1	22~28	1	22~28
IPTV	3~7Mbit/s	1	3~7	3	9~21	2	6~14
家庭剧院数字音频系统	5.4Mbit/s	1	5.4	1	5.4	1	5.4
数字音频 CD	2×0.8Mbit/s					3	4.8
基于 IP 的电话	(0.064+0.016)=80 kbit/s(codecG.711)	2	0.16	2	0.16	3	0.24
IP 数据	2Mbit/s	2	4	2	4	5	10
总计		6	34.5~44.4	9	40.6~58.4	15	48.4~62.2

6.2 PLC局域网

最明显和最普遍的就是用PLC在公共领域和专用领域中建立一个局域计算机网络。一些家庭一直热衷于在家中安装几台个人计算机（PC），共享一系列应用，专用领域则期望传输一些专用信息或因特网应用。

6.2.1 网络连接共享

最常见的PLC应用是实现在同一网络中一些终端设备和计算机之间的网络共享。

PLC技术可以轻松地把各种家用和商用计算机通过电力网络连接到因特网的调制解调器。网络的体系结构具体如图6.4所示。通过由电力网络，PLC设备续传信号，实现PC与网络的连接。PLC最主要的优点之一就是家中任何插座都可以检索到网络信号。

在图6.4中，连接到宽带网络中的各个用户都共享传输速率。

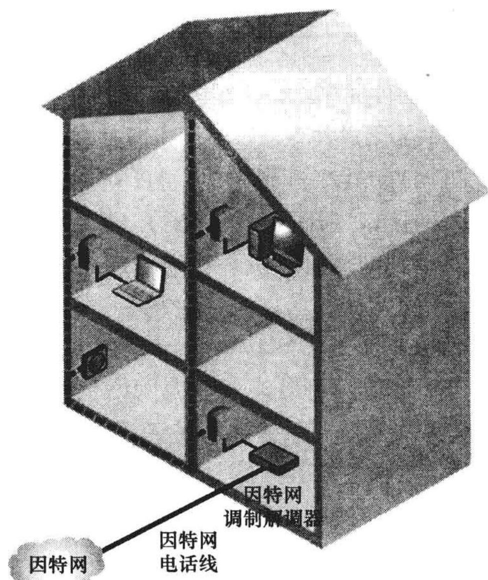


图6.4 网络连接共享

6.2.2 文件和打印机共享

PLC 局域网络可以将有线或无线连接的用户网或专业计算机网络中的所有应用有机连接起来。

文件和打印机共享应用是两个最频繁的应用（见图 6.5）：

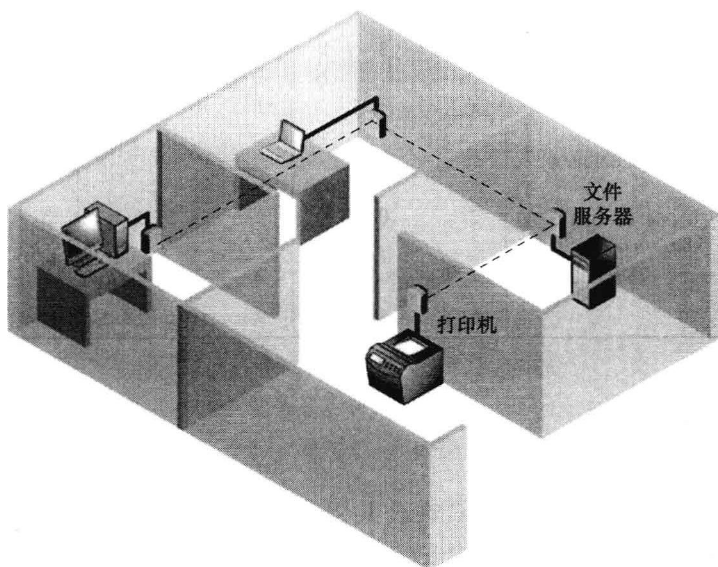


图 6.5 PLC 局域网中的文件和打印机共享

1）文件共享：一个服务器通过一个 PLC 设备连接到电力网络后，主机的文件就被在网络中的用户共享。这些用户通过电力网络连接到服务器并且正确配置到 PLC 设备。

2）打印共享：同样地，打印机能放置在家中或办公室中任何有利位置，并通过以太网接口（RJ-45 连接器）连接到 PLC 网络，然后其他用户可以通过 IP 地址设置连接到网络打印机。

6.2.3 音频广播

PLC 局域网可以通过电力网络传输音频数据（见图 6.6），音频数据源主要包括以下几种：

1）音频文件服务器。MP3 或 WAV 格式的文件通过电力网络传送，用 PLC 设备续传后，连接到装有 Hi-Fi 的设备。

2）Hi-Fi 系统。从一个 Hi-Fi 系统连接到另一个 Hi-Fi 系统或连接到音频扬声器系统的音频信号可以被共享。在第 2 种情况中，电力网络取代了音响系统和音频扬声器之间的连接电缆。

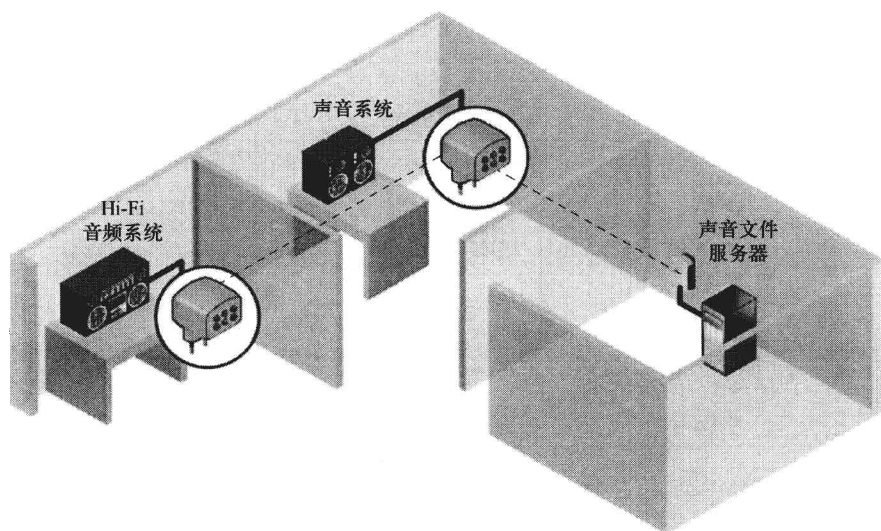


图6.6 PLC网络中的音频广播

6.2.4 娱乐应用

越来越多的娱乐应用（视频游戏）通过计算机网络连接到联网中的各个玩家。游戏终端可以用电力网络给装配到网络接口，这种连接目的与用PLC局域网的文件共享其实是一样的。

6.2.5 视频监控

广泛使用的网络摄像机被装置到以太网接口就意味着它们能经由插座连接到PLC局域网。这样安放摄像机的地点就灵活得多，只要有插座的地方附近就行。对于这个应用可以详见图6.7。

6.2.6 作为Wi-Fi网络的骨干

我们将在第13章（专用于混合网络）中看到，每个计算机网络技术都有其自身的优点和缺点。

在建立了Wi-Fi网络的大楼内，无线计算机网络为用户提供了灵敏性和弹性。然而，由于这个技术的硬件制约，需要使用有线的以太骨干网覆盖整个大楼。作为骨干网的以太网实际上可以采用PLC局域网来代替，也就是将Wi-Fi接入点连接至电力网络上。

图6.8表示的是这种网络类型的架构，每个Wi-Fi接入点形成了一个用PLC设备连接网络的无线单元。

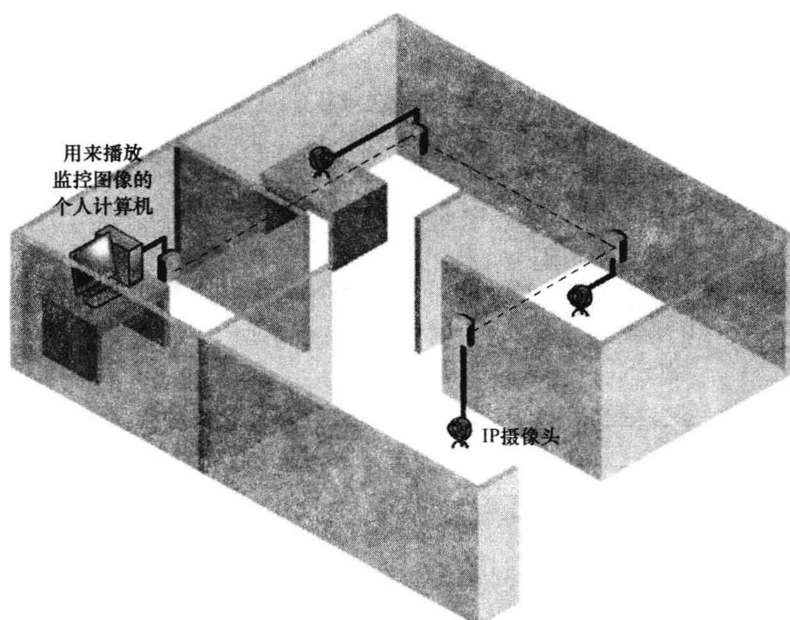


图 6.7　PLC 网络中的视频监控

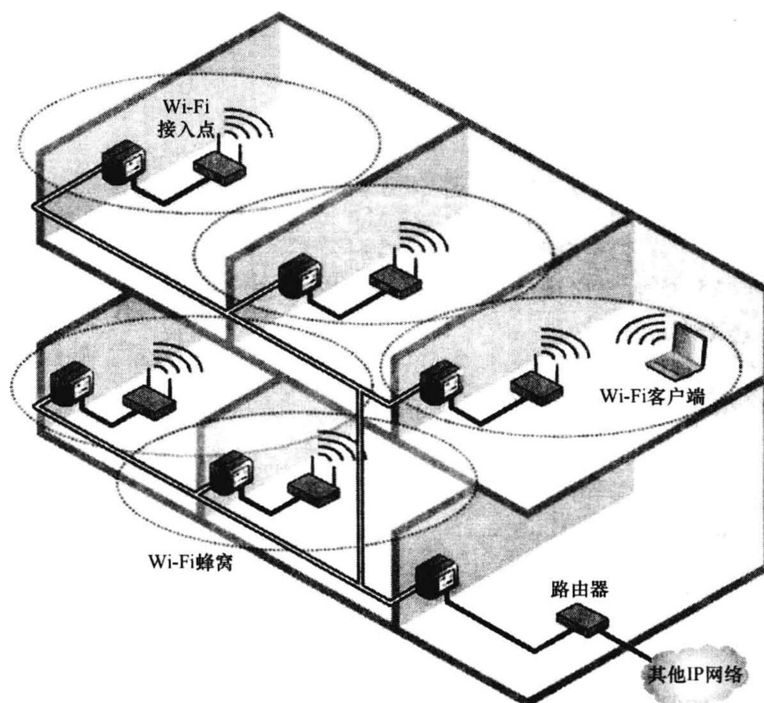


图 6.8　PLC 本地区域网络作为 Wi－Fi 网络的主干网

6.3 网际网络资讯接收器（InternetBox）和 PLC

欧洲的很多因特网接入服务供应商，诸如 Orange、Free、Neuf-Cegetel、Alice、Club-Internet、Vodafone、Belgacom；美国的 Comcast；或者日本的 NTT 公司等，他们都提供了通过 InternetBox 接入因特网“multiplay”业务（服务）的解决方案，主要包括：

1）数据：InternetBox 说到底就是一个接入网络的调制解调器，能使用户接入数据服务器，诸如 Web、报文发送、FTP、IRC、P2P 等。

2）语音。IP 电话（Telephony over IP services）。InternetBox 此时很像一个电话终端，其工作机理很像连接到 STN（Switched Telecommunications Network）上的模拟电话。

3）视频。用于在 IP 网络广播电视节目的 IPTV（网络数字电视）和 VoD（Video on Demand）。

4）IP 业务。家庭移动电话，家庭自动化（如电力管理和家庭服务器）等。不久，这些业务将使得 InternetBox 成为一个真正智能的网关。

这些服务的每一项必须经由以太网连接到终端用户（如电视、电话、计算机、IP 家用电器等），PLC 局域网使用这些既有的网络，因此是一个不错的解决方案。

图 6.9 表示这些服务需要 InternetBox 和视频解码器或电话之间建立以太网连

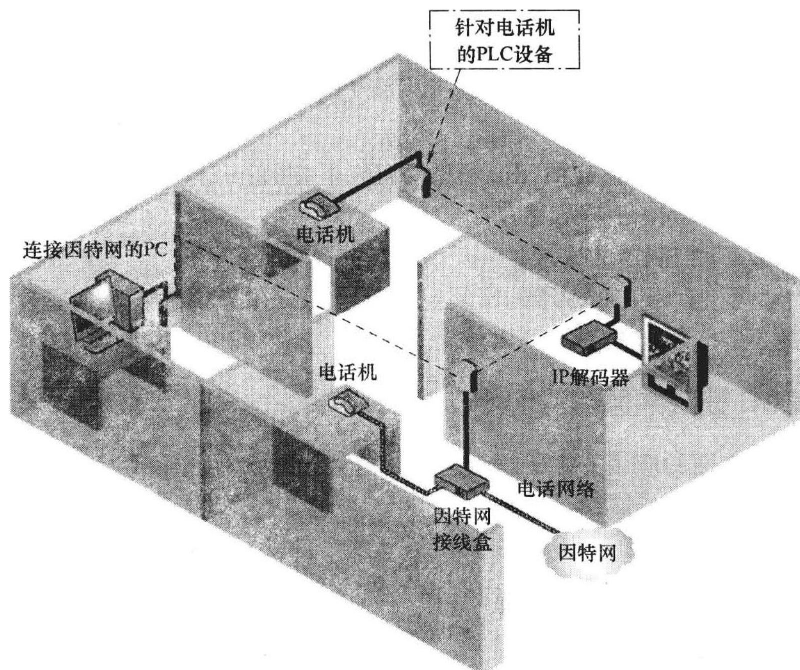


图 6.9 因特网终端和 PLC

接，这个链路可以由 PLC 设备提供。

因特网接入服务提供商已经提供了下列集成了 PLC 的产品，或者提供了完全由他们制造的产品。

- 机顶盒；
- TV 解码器；
- 电气插头；
- 平板显示器。

6.4 PLC 的新应用

随着 PLC 技术的成熟，一些制造商开始考虑使用 PLC 作为传输媒介，特别是那些至今还没有网络的地方，或者是那些只有私人网络以及昂贵网络的地方。

实际上，随着工业设备数量的增长，有因特网接入服务就有可能建立允许连接的新型网络（尤其是在船上、公共领域和汽车上）。

6.4.1 PLC 的工业应用

工业领域比公共领域或者专业局域网对网络的要求更为严格，因此工业领域网络应用的局限性就更为严重。迄今为止，这些制约（局限性）已经影响到了 PLC 的发展。不过随着 HomePlug 的成熟以及 PLC 网络应用的先驱者们反馈的信息推动了 PLC 技术的发展，并且使人们开始考虑将 PLC 作为设备之间连接的一个技术解决方案。

现在 PLC 网络在工业方面的应用主要有以下方面：

1）传感器网络；

2）可编程序控制器的连接；

3）当计算机置于布线困难的密闭空间时（如在探头顶部或有金属管道的空间而无法使用 Wi-Fi 的时候等）。

6.4.2 PLC 在公共领域的应用

像在工业方面的应用一样，越来越多的公共领域已有通信或者安装了以太网接口的设备准备连接到局域网。

很多应用已经运用了 PLC 来连接设备，尤其是以下几个方面：

1）面向互动终端的内容发布；

2）饮料分配情况的信息反馈；

3）出勤打卡机的数据验证。

6.4.3 同轴电缆PLC

在第7章可以看到，PLC设备不仅可以用110或220V、50或60Hz的电线而且还可以用其他传送1~30MHz信号带宽类型的线路。一种被PLC设备广泛运用的线路就是同轴电缆（原本是电缆公司传递电视节目的有线电视信道）。

这类电缆具有非常好的传播特性和抗干扰能力，可以用于PLC信号传输。因此，在建立PLC网络的时候，同轴电缆可以弥补仅使用电力网络带来的网络拓扑等方面的某些不足（例如电力网络过于陈旧，再如对需要开展的应用而言，电力网络可能太过复杂等）。

不用电流的PLC

通过用电缆传送PLC信号不需要110或220V、50或60Hz的电力信号。只要PLC设备不论采用什么方式都可以由电池供电，那么PLC在楼宇内就算没电的情况下也可以使用。下面要做的，就是利用电力网络彼此通信，但是不能断掉它们的电源。这种看似原始的PLC应用被证明是很有实用价值的，特别是当电力网络被切断的时候，安装有特殊电池的PLC设备此时仍旧可以完成通信工作。

6.4.4 PLC在机动车中的应用

机动车的增长需要各种控制和仪表盘之间的内部数据传输。这些数据交换需要的数据线加起来长达3km，重约50kg。

在欧洲，Valeo零件制造商和PLC产品制造公司联合起来，利用PLC实现车载传感器到仪表盘的信息交流。

这种类型的PLC网络也可以用于外置摄像机或者机载DVD视频设备上。

6.5 经济效益

在本章中我们看到大多数使用PLC并进行传输的应用需要面对的PLC固有的制约（如传输速率、拓扑图以及网络中的用户数量）。

上述应用的数量正在不断地增长，不过大多数已经能在传统的网络中得以实现（如语音和视频）。

PLC终端设备的数量也在不断地增加，而且，在那些销售数据处理设备和网络设备的零售商那里，也能够觅得PLC产品的身影。

因此，不仅应将PLC视为一种网络技术，而且还应当将其视为通过信息共享来连接各类设备的一种简单的方法。PLC出现在Hi-Fi领域就是一个显著的例子。连接网络的中心服务器能够通过由PLC连接的局域网将任何形式的数据流（如视

频或音频）传送到家中的任何设备上去。

因此 PLC 网络的经济效益是非常高的，特别是在以下几个方面：

1）在 2009 年，HomePlug AV 的产品问世。

2）因特网接入服务供应商承诺将 InternetBox 的服务扩展到住宅，并由此将培育公共领域的 PLC 用户群。

3）公共领域对这项技术的理解不断深入，特别是这项技术的应用十分简单（没有新的布线，用现有的插座、简化的配置、安全等）。

4）专业应用领域的人士对 PLC 网络的理解不断深入，认识到 PLC 网络是电缆和 Wi-Fi 的有机补充，特别是符合专业应用网络管理和监督要求的那些 PLC 产品不断推陈出新。

图 6.10 表示到 2010 年 PLC 网络的增长情况。设备成本的低廉以及与不同技术（网关、路由、调制解调器、防火墙和服务器等）相融合的产品不断推陈出新无疑将使这一技术前景一片光明。

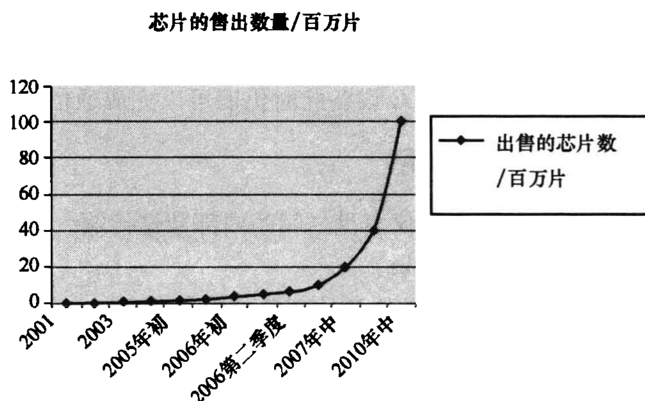


图 6.10 全球售出的 HomePlug 芯片数量图

第7章　设　　备

自2003年HomePlug1.0规范发布以来，PLC网络的设备市场就一直在不断成长。该市场从最初关注于低传输速率和少量计算机组成的小型网络，已经转向面对热衷于在因特网接入服务提供商的支持下，可以实现因特网连接共享而又消除了布线约束，且保持相对易用性的技术的私营个体企业。

本章将介绍当前市场中出现的所有PLC产品，这些产品可以将终端设备连接至本地局域网，构建或者优化PLC网络（滤波器、中继器、注入器等）。

7.1　PLC技术

自第一个高速PLC设备出现以来，已经成功地开发了多种技术，但是，目前为止，还没有任何相关国际标准。

在向公众推广的技术之中，有几种方法已经实施，尤其是：网络模式的选择，调制技术，子带数量，MAC层的实现。

HomePlug技术广为大众所接受，其产品占据了PLC设备市场份额的90%以上，因此正在成为标准产品。

表7.1中根据所选择的网络模式，对各种PLC技术进行了小结。

表7.1　按照网络模式进行分类的电力线通信技术

<table>
<tr><th colspan="2">技　术</th><th>模　式</th></tr>
<tr><td colspan="2">Ascom APA 450（4.5Mbit/s）</td><td>主-从</td></tr>
<tr><td colspan="2">Itran（Main. net）PLTNet&ITM1（2Mbit/s）</td><td>主-从</td></tr>
<tr><td rowspan="3">HomePlug</td><td>1.0</td><td>点对点</td></tr>
<tr><td>1.0 Turbo</td><td>点对点</td></tr>
<tr><td>AV</td><td>中心式</td></tr>
<tr><td rowspan="2">DS2</td><td>DSS4200（45Mbit/s）</td><td>点对点</td></tr>
<tr><td>200Mbit/s</td><td>主-从</td></tr>
<tr><td rowspan="2">Spidcom</td><td>45Mbit/s</td><td>点对点</td></tr>
<tr><td>SPC200（200Mbit/s）</td><td>主-从</td></tr>
</table>

根据各个应用的限制条件，PLC技术可以使用各种不同的网络模式（主-从模式、点对点模式和中心模式等）。Ascom和Itran是最早开发基于以太网接口的PLC

设备的两家公司。最初，这两个公司都偏好主-从模式，因为这种模式具备集中管理功能。

7.1.1 主-从模式

图7.1展示了主-从模式低压（LV）PLC网络的架构。我们可以发现主设备在MV/LV（中压至低压）电压级，该设备可以检测PLC网络工作状态的正常与否，特别是检测位于建筑物电能表之间的从设备间的已有网络连接是否正常。

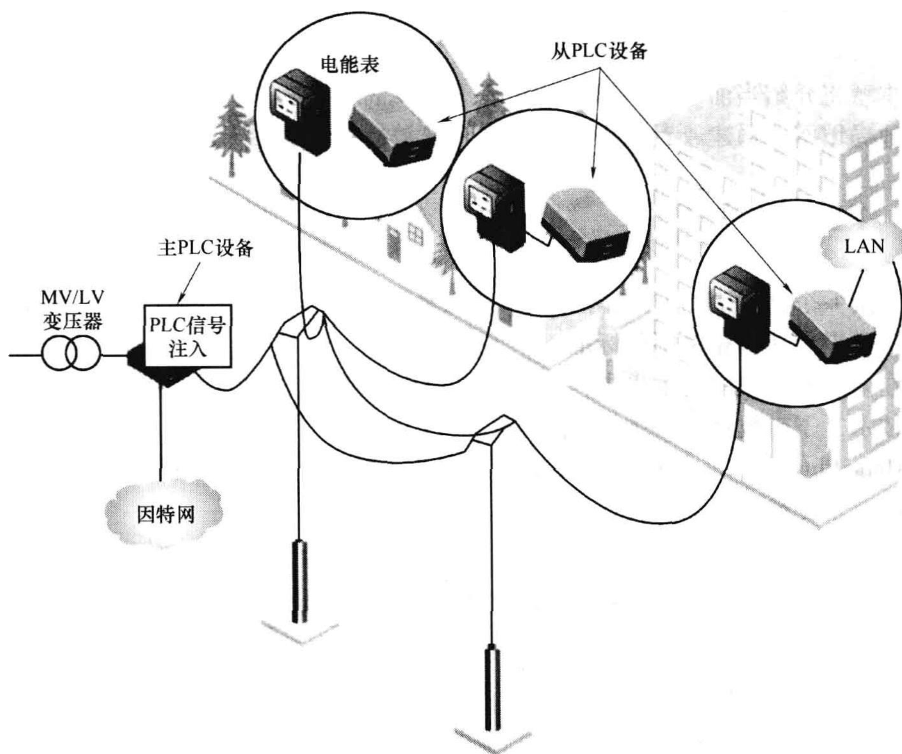


图7.1 主-从模式架构简图

图7.2为用于家庭电线网络的另一种主-从模式的架构。在图中，我们可以发现第2章中曾经介绍的传统的私人电力网络设备。

电气配电盘可以控制布线、电源插座、照明灯泡和电气设备等。通常，将连接至电气配电盘的电缆称为“总线-汇流电气连接”，因为，它们从中心点（电气配电盘）出发，按照供电需求，遍布整个建筑物。

使用这种拓扑时，PLC主设备的理想安装位置就是该中心点（电气配电盘）。从设备由沿着电力网络四处分布的插座组成。

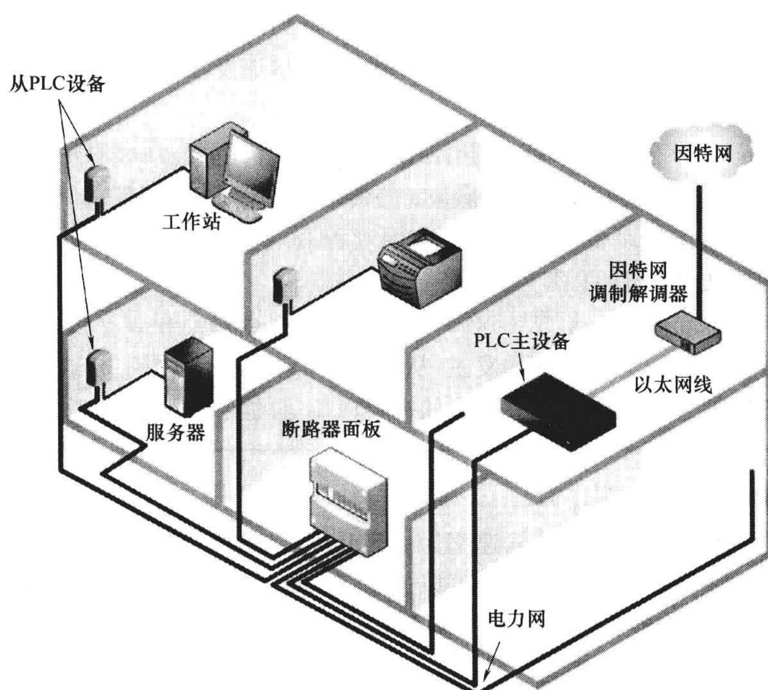


图7.2　主-从模式家用低压PLC网络的设备布置示意图

主设备充当固定电话网（例如，可以连接至调制解调器，以接入因特网）和PLC本地局域网之间的网关，而PLC本地局域网则使用建筑物内部的电力网络。此外，该设备也负责整个（本地局域）网络和各种从设备的管理工作。

表7.2对采用总线-汇流电气连接方式的主要优点与缺点进行了小结。

表7.2　使用数个总线-汇流电气连接的优点与缺点

总线-汇接电器连接的数量	优　点	缺　点
单个总线-汇流连接	设计容易 主设备潜在重复性 监管更加容易	带宽呈划分状态 数据帧可以存在多个传输路径 可能存在循环回路
多个总线-汇流连接	网络覆盖能力更广、更强 可以实现重要网络之间的隔离	监管工作较复杂

大量PLC设备生产商选用了主-从模式，其中，著名的有：

1）Main. net。公共低压电网产品开发商。该公司优先考虑主-从模式，以与电力网络拓扑相匹配。

从传统的角度看，这是一种星形拓扑。作为 PLC 信号注入点，MV/LV 变压器位于星形拓扑的中心，终端用户 PLC 设备则位于从该变压器出发的各个总线-汇流电气连接的端点处。

2）Ascom。该公司自 1998 年起使用该模式开始着手公共和家用低压电网产品的研发。这一代产品可以提供 250kbit/s 的传输速率。其中，有一个设备用作主设备，其他的则用作从设备。配置可以使用远程登录模式（Telnet Mode）完成，也可以采用配置文件和 TFTP 客户端-服务器系统。

3）DS2 和 Spidcom。早先，这两家公司均使用点对点模式，实现了系统部署的简化，目前，它们均致力于开发主-从模式产品，充分利用中心式管理的优势和更佳的服务质量管理功能，以实现诸如视频应用等的实时应用 TDMA 帧分配功能。

Ascom APA 设备实例

Ascom APA 设备的工作传输速率为 4.5Mbit/s，是最早的第一代高速 PLC 设备的代表性产品之一。对于主设备，可以通过 Telnet 协议访问并完成设备配置工作，此后，还可以使用 v2/v3 SNMP 管理控制台进行监控。主设备可以管理多达 63 个从设备。

图 7.3 ~ 图 7.6 为 Ascom APM45 主设备和从设备。

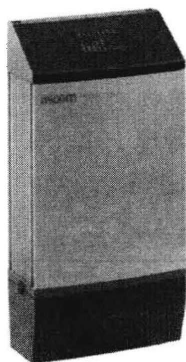


图 7.3　主设备（负责管理 Ascom Powerline APM-45oPLC 网络）

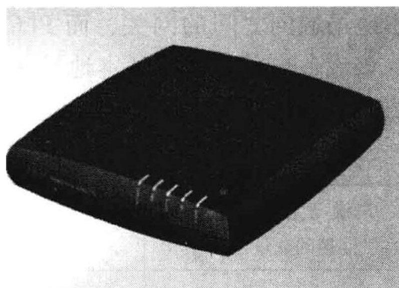


图 7.4　Ascom Powerline APA-45i 从设备（用于将客户机终端连接至电力线局域网）

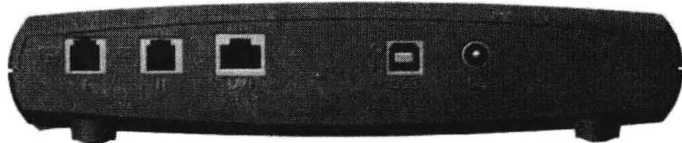


图 7.5　从设备的接口

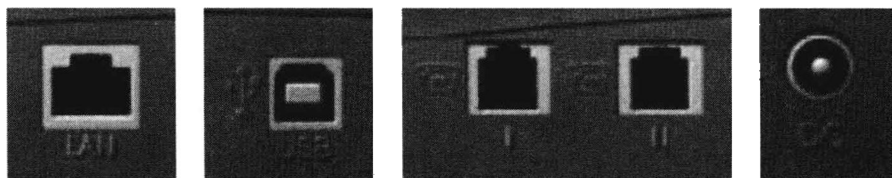


图7.6 从设备的RJ-45、USB和RJ-11以太局域网接口

某些PLC设备可以用作PLC网络上的远程电话接口。例如，Phonex公司开发的带有RJ-11接口的此类设备，就可以实现电力网络上的语音模拟通信。

7.1.2 点对点模式

在主-从模式中，主设备处于较高的层级（它负责网络的管理和控制功能），从设备则处于较低的层级（它们的功能仅仅限于与主设备进行通信）。在点对点模式中，所有设备层级相同，并可与网络中的所有其他PLC设备交换数据。因此，这类网络有$N \times N$个链路。

由于LAN架构中，任何一个终端（典型为PC）都必须能与其他任意LAN终端交换数据，因此，从图7.7可知，点对点模式很好地适用于局域网络。HomePlug1.0和Turbo使用这种工作模式。

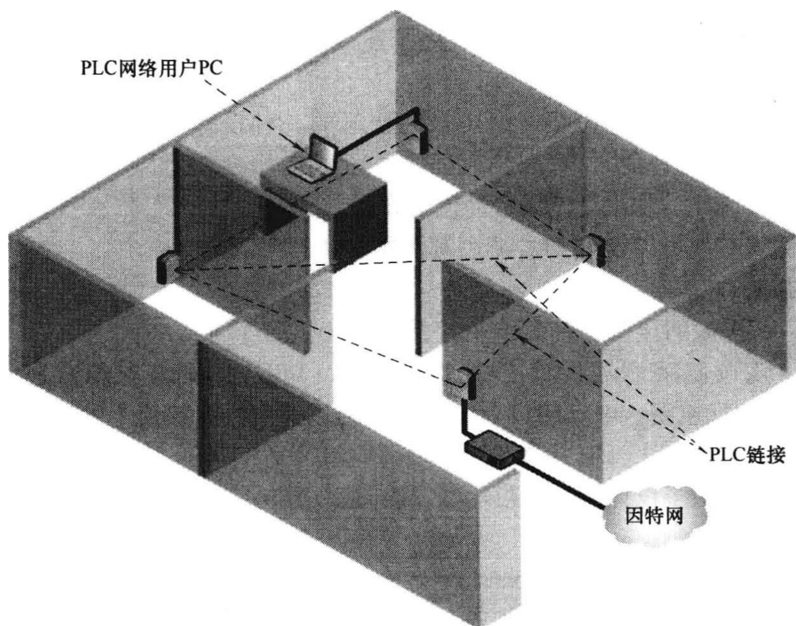


图7.7 点对点模式PLC网络的架构

7.1.3 中心模式

如第3章所述，HomePlug AV 使用了中心模式，该模式组合了主-从模式和点对点模式的优点。

在 HomePlug AV PLC 网络中，其中，有一个设备充当中心设备，负责管理网络中 PLC 工作站之间的通信。PLC 工作站之间的数据交换可以直接进行，无需经过该中心设备。然而，工作站必须由中心设备完成身份确认，并遵守中心设备分配给它们的工作时间。

7.2 PLC 调制解调器

PLC 技术本质上使用了电力网络，因此，无论是哪一种类型的 PLC 设备，都必须连接至插座或者直接将信号注入电力线之内。使用信号注入技术，可以将 PLC 设备直接连接至电力线之上，关于信号注入，本章后面将进一步描述。

PLC 技术并不使用调制解调器实现的调制-解调功能，我们所谈到的 PLC 调制解调器是指需要接入 PLC 网络的终端所连接的设备。

与 Wi-Fi 接口不同的是，Wi-Fi 接口以电路板的形式集成在终端之内，而 PLC 接口则没有采用终端内集成这种方式。因此，终端（大多数情况下为计算机）所连接的设备拥有两个接口：一个接口用于连接电力网络；另一个接口（RJ-45 或 USB）则用于连接终端。

PLC 调制解调器是电力线网络内最为普遍的一种设备，看起来像一种标准电器。它配装有一个公插头，可以插入插座；还配有 USB 或者以太网接口，可以连接某个终端，因此，它也是使用最简便的设备。

从外侧观察，可以发现 PLC 调制解调器有如下两个接口：

- 公插头；
- RJ-45 以太网接口或者 USB 网络接口。

通常，该调制解调器设计有3个指示器（LED），用来向用户显示110或220V/50或60Hz电源、电气接口上的 PLC 信号以及 RJ-45 接口上的以太网 PLC 信号（见图7.8左图）。

某些设备上最多设计有5个指示器，此时，用户可以检查设备是否处于正常的工作状态。

PLC 调制解调器的散热

最初的 HomePlug1.0 PLC 设备使用塑料外壳，设备长期工作于输入电压110或200V/50或60Hz时，存在散热问题。这种外壳可能导致无法长期工作于高温状态

的电子元器件失效。现在，这种 PLC 设备已经进行了改进设计，采用了更加可靠的元器件、散热器和通风口设计（见图 7.8 右图）。

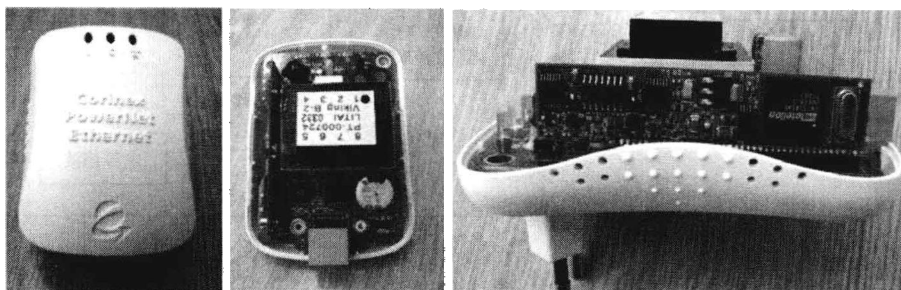


图 7.8 HomePlug Corinex Power Net PLC 调制解调器的外观和内观详图

无论是塑料外壳的消费电子设备还是金属外壳的专业型设备，即使叠放在通风不良的环境且环境温度高达 70℃时，这些设备也可以正常地工作。

在机壳内，整个硬件结构均以主组件为中心进行设计（HomePlug PLC 芯片，见图 7.8 中图）。Intellon 公司为 HomePlug 芯片的主要供应商。

表 7.3 简要列出了随着 HomePlug 技术的进展而出现的各种不同型号的芯片。

表 7.3 Intellon 公司芯片的型号

Home Plug	芯 片
1.0（也名为 1.0.1）	INT5130、INT51MX
Turbo（也名为 1.1）	INT5500
AV	INT6000、INT6300

这类 PLC 芯片可以实现第 3 章所描述的所有 PLC 网络功能。以该芯片为中心，使用了大量元器件和电子电路，对 PLC 调制解调器进行了进一步的优化：

1）优化了与电力网络的连接性能（即 PLC 调制解调器连接至电力网络）。

2）实现了 PLC 信号增益控制，对数据的发送/接收进行了最优化，充分考虑了各种不利条件，尤其是电力网络上的噪声影响。

3）实现了与 PLC 网络状态有关信息的存储功能。该功能通过 EPROM（调制解调器重启时不会丢失信息的永久性存储器）和 SRAM（非永久性存储器，调制解调器重启时，信息会被擦除）实现，可以存储与 PLC 链路、网络加密密钥或者存取权限等有关的信息。

图 7.9 为 HomePlug1.0 PLC 调制解调器的硬件结构示意图。

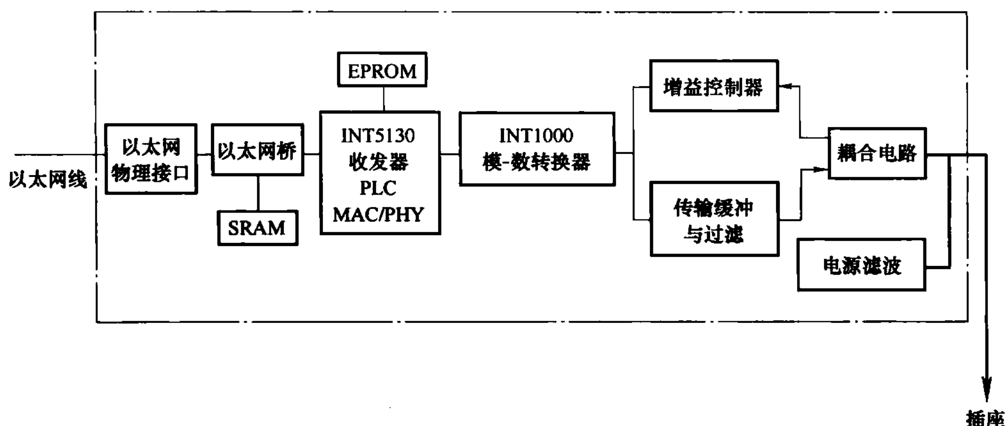


图 7.9 PLC 调制解调器的硬件结构图

该制造商已经开发了两种类型的 PLC 调制解调器：桌面型调制解调器，可以放置在桌面或者底座上，通过一根电缆连接至插座；墙装型调制解调器，该调制解调器采用集成式外壳，可以直接插在插座上。墙装型调制调解器使用起来极为方便，因此，大多数 PLC 调制解调器都为墙装型。

图 7.10 为墙装型（左图）和桌面型（右图）调制解调器的实物图。

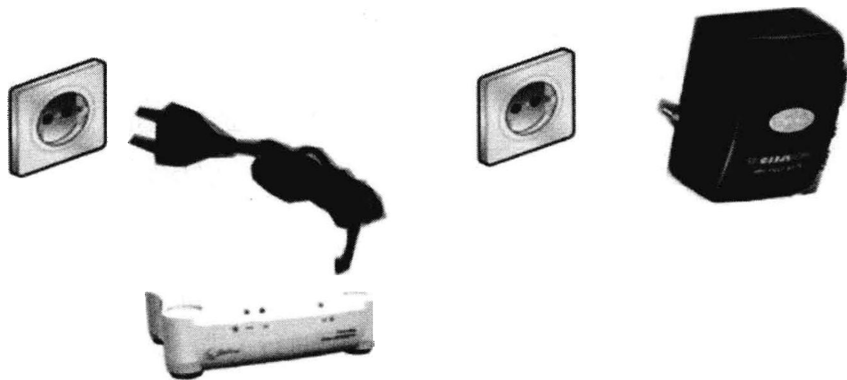


图 7.10 墙装型和桌面型 PLC 调制解调器

7.2.1 USB 接口的 PLC 调制解调器

USB 接口的 PLC 调制解调器配设有一个 USB 接口，因此，可以直接连接至计算机或者网络终端设备的 USB 接口上。该 USB 接口可以充当虚拟的网络接口卡，能够实现与 PLC 网络的连接。这类调制解调器令人感兴趣的一点是，即便实际工作的所有计算机均没有网络接口卡，但是却全部配有 USB 接口。然而，与以太网

PLC调制解调器的配置工作相比，该类调制解调器的配置工作却没那么容易。

图7.11为一种F@ st Plug型Sagem USB-PLC调制解调器。



图7.11 F@ st Plug型Sagem USBPLC调制解调器

7.2.2 PLC以太网调制解调器

计算机内、网络终端设备、电子设备以及家用电器等的常用网卡，在以太网电路板上配有RJ-45接口，进一步简化了网络的构建工作。

这种类型的调制解调器已经在PLC设备中得到了最广泛的使用。除了使用和配置极为简单之外，其价格也越来越便宜。图7.12为dLAN85型高速以太网Devolo以太网PLC调制解调器。对于HomePlug 1.0调制解调器，PLC调制解调器以太网接口卡最初使用10baseT（10Mbit/s）标准，MAC层的最大有用带宽高达8.2Mbit/s。此后，在HomePlug Turbo和AV调制解调器中，使用了100baseT（100Mbit/s）标准。

HomePlug PLC设备的性能提升有可能驱使制造商使用1000baseT（1000Mbit/s）标准接口板，以突破以太网接口数据吞吐率的限制。因此，如果出现了光纤PLC设备，也不是什么令人惊奇的事情。Devolo可以提供带有两个USB接口和以太网接口的设备。

图7.13为dLAN双接口型Devolo PLC调制解调器，该设备配有USB接口和以太网接口。



图7.12 dLAN85型高速以太网Devolo以太网PLC调制解调器



图7.13 dLAN双接口型Devolo PLC调制解调器（该设备配有USB接口和以太网接口）

图7.14为符合HomePlug AV标准的Devolo PLC调制解调器。其中，左图为消费性墙装型；中图为专业桌面型；右图则为带有以太网和USB接口的专业墙装型。



图7.14 Devolo HomePlug AV PLC设备

7.2.3 PLC有线电视调制解调器

某些PLC调制解调器生产商还提供可以连接有线电视网络的PLC设备。这类设备具备极强的抗电磁干扰能力。有线电视使用了以下两种频带：

1）频带：1~24MHz，用于数据；

2）频带：47~862MHz，用于电视信号。

与电力网络相比，有线电视运营商的网络要小得多，通常情况下，有线电视插座的数量也仅仅只有少数几个。然而，有线电视网络拥有相对恒定的速度，且任何情况下，性能均更加稳定，因此，电力网络出现意外的情况下，有线电视网络可以发挥良好的替补作用。

有线电视网络是一种公用网络，因此，其速度按介质所连接的用户数量平均分配给各个用户。

PLC有线电视设备可以使用多种类型的连接器，尤其是用于连接有线电视的F-type连接器。对于有线电视网络来说，通常，传输距离为500~700m时，仍然保持较高的可用数据吞吐量。

图7.15中自左向右分别为Corinex CableLAN有线电视PLC调制解调器、同轴电缆、F-type连接器和视频分配器。

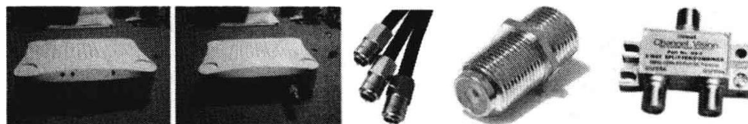


图7.15 Corinex CableLAN有线电视PLC调制解调器、同轴电缆、F-type连接器和视频分配器

HomePlug技术及其传输速率发展的同时，PLC有线电视调制解调器也在同步发展。这些调制解调器可以用于以下两类应用：

1）实现有线电视网络上的数据传输，并使其成为PLC网络的骨干网络；

2）使用带有适配器的同轴电缆接口，即所谓的“注入器”（参见本章后续内容），将PLC信号直接发送至电力线而无需使用插座。

尽管这些 PLC 调制解调器使用了非电线介质，通过诸如 HomePNA（家庭电话线网络联盟）或者 UPA（通用电力线协会）等的 HomeNetworking 技术，还是很好地实现了与 HomePlug 的兼容。表 7.4 按技术列出了主要的 PLC 有线电视调制解调器的传输速率。

表 7.4　主要的 PLC 有线电视调制解调器的传输速率

PLC 有线电视调制解调器	技　术	传输速率/(Mbit/s)
Corinex CableLAN	HomePNA 1.0	10
Corinex CableLAN AV	HomePNA 3.0	128
Corinex CableLAN 200	Pre-UPA	200

HomePNA 标准也支持通过家用电话线实现数据传输。Corinex 公司特地向市场推出了 CableLAN Combo 适配器产品，该产品使用 HomePNA 3.0 标准，并拥有两个接口，即同轴电缆接口（F-type 连接器）和电话接口（RJ-11 连接器）。

7.2.4　电源插座集成式 PLC 调制解调器

某些生产商生产的 PLC 调制解调器直接集成了电源插座。

Lea 和 Legrand 公司开发了一种 PLC 插座，即所谓的“智能插座”。通过该产品，它们成功地将 HomePlug PLC 调制解调器集成进插座单元和以太网 RJ-45 连接器内。该智能插座的接线图如图 7.16 所示。

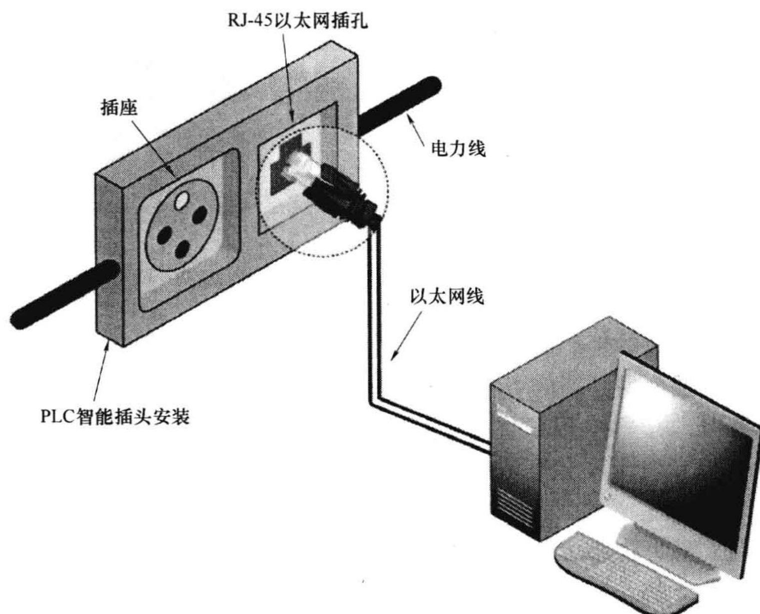


图 7.16　Lea-Legrand SmartPlug PLC 插座工作示意图

7.2.5 PLC/Wi-Fi 调制解调器

第13章将专门描述混合型网络。该章中，我们可以看到，PLC 和 Wi-Fi 技术具备完美的互补特性，可以构建拥有最优无线信号覆盖性能的复杂网络。作为 Wi-Fi 网络的骨干部分，PLC 网络可以进一步提高 Wi-Fi 网络的无线信号覆盖性能。

HomePlug 技术的最新进展，使得该技术的性能可以与这两种技术相媲美。HomePlug Turbo 可以在物理层提供的最大有用吞吐量为 85Mbit/s，而 IEEE802.11g 标准则为 55Mbit/s。PLC/Wi-Fi 设备则充分地结合了 PLC 的易用性和 Wi-Fi 的移动性。

这些设备中，某些设备整合了 PLC 和 Wi-Fi 组件，而另外一些设备则在 PLC 调制解调器内提供有 PCMCIA 插槽，据此，用户可以使她/他的无线网络拥有性能最优的 Wi-Fi 功能。

图7.17为 Thesys 调制解调器（左图）和 Devolo MicroLink dLAN 无线式（右图）PLC/Wi-Fi 调制解调器。

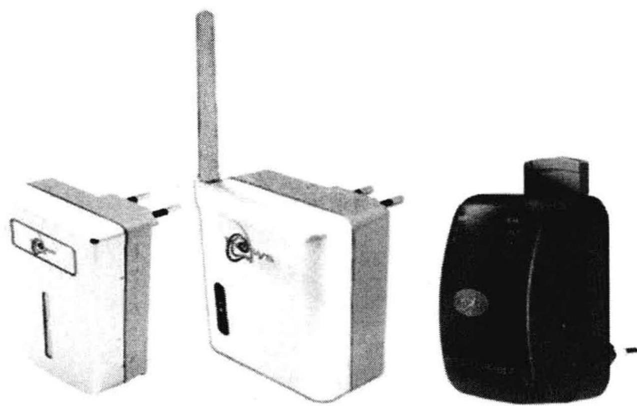


图7.17 Thesys 和 Devolo MicroLink dLAN 无线式 PLC/Wi-Fi 调制解调器

目前，相当数量的生产商正在努力优化处于 PLC 和 Wi-Fi 之间的 MAC 层，以进一步提高这类混合型网络的可靠性和 MAC 层的性能，这些项目于2009年推出市场化产品。其中，有一种 PLC 优化应用是 Wi-Fi 的补充。该应用由采用建筑物照明系统构建的 PLC 骨干网和灯泡周边就近布置的 PLC/Wi-Fi 设备组成。

中国台湾省的建兴公司开发了一种 ORB 产品。该产品外观如同一个 Wi-Fi PLC 灯泡，除了照明功能之外，还可以将 Wi-Fi 无线电信号传输至室内每一个角落。该灯泡是一个 PLC 设备，不仅连接照明系统，也连接至照明系统和供电系统上的其他 PLC 或 PLC/Wi-Fi 设备。

7.2.6 多功能 PLC 调制解调器

某些 PLC 产品具备各种不同的网络功能，可以满足网络工程师与用户的不同需求。在这些产品中，典型的有：

1）以太网 PLC/集线器调制解调器，用于将多个 PC 连接至同一个 PLC 以太网调制解调器上。

2）ADSL/路由器 PLC 调制解调器，用于在电力线网络上发送源自因特网连接的信号。某些设备甚至另外添加了一块 Wi-Fi 驱动板。

图 7.18 为 Hub Netgear（左图）和 Thesys NetPlug（右图）PLC 调制解调器。

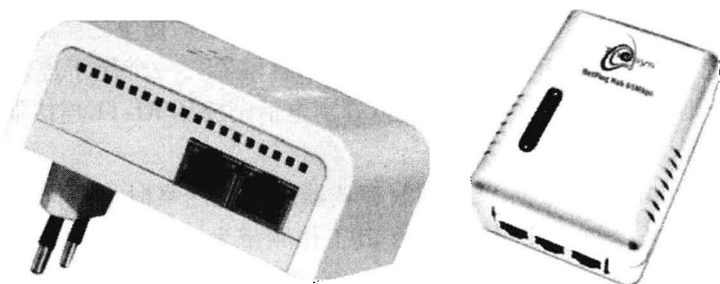


图 7.18 Hub Netgear 和 Thesys NetPlug PLC 调制解调器

图 7.19 为 Devolo dLAN ADSL 调制解调器的路由器 PLC 设备。



图 7.19 Devolo dLAN ADSL 调制解调器的路由器 PLC 设备

7.2.7 PLC 音频和电话调制解调器

由于 PLC 可以在电力网络上传输数据，因此，很长时间以来，某些生产商就一直致力于开发音频和电话 PLC 产品。

音频 PLC 调制解调器的某一个侧面，可以连接电力网络，同时，在另一个侧

面上，还可以连接诸如音频扬声器、音频系统、音频文件服务器等 Hi-Fi 设备。

图 7.20 为 Devolo MicroLink dLAN 音频 PLC 调制解调器。该调制解调器配有 Cinch（两个用于输出通道，两个用于输入通道）、SPDIF（一个用于输入通道，一个用于输出通道）、音频插座（一个用于输入通道，一个用于输出通道）连接器，可以通过电力网络广播四路 192kbit/s 音频信号。

必须对音频 PLC 调制解调器进行配置，完成 PLC 局域网组件的参数化工作，并加载文件服务器所需要的插件。

在建筑物内，通常仅能找到 1～2 个用于连接公用 STN 的电话插座，此时，也可以使用 PLC 实现建筑物内电话模拟信号的传输工作。据此，可以方便地使用所有房间内的电力网络，实现远程电话插座与本地现有电话插座之间的连接。

这种情况下，需要使用两个电话 PLC 调制解调器：一个用于连接电信的入户馈线；另一个则用于连接某个插座。模拟蜂窝电话则使用 RJ-11 连接器，连接至第二个调制解调器。

图 7.21 为 Wingoline 电话 PLC 调制解调器。构建网络时，在同一个电力网络上最多可以使用 24 个该型调制解调器，其工作频带为 3.3～8.2MHz，信号在电缆上的传输距离为 150m（比以太网 PLC 调制解调器稍短）。

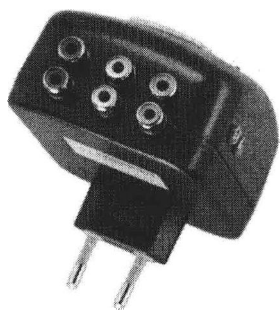


图 7.20 Devolo MicroLink dLAN 音频 PLC 调制解调器

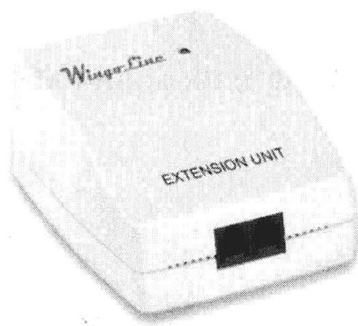


图 7.21 Wingoline 电话 PLC 调制解调器（带有两个 RJ-11 电话插座）

7.3 介质接入方法

在 PLC 网络中，必须采用介质接入方法，实现 PLC 设备与电力网络之间的连接，以获得物理层的最佳性能并因而可以在较高层级获得最佳的可用数据吞吐量。

需要将 PLC 设备连接至电力网络时，可以使用两种不同的方法（也称耦合方法）：容性耦合和感性耦合。

大多数 PLC 调制解调器均使用容性耦合方法。术语“容性”表示连接至插座

的 PLC 调制解调器可以视作一个电容（即电容器）。图 7.22 为容性耦合的工作原理简图。

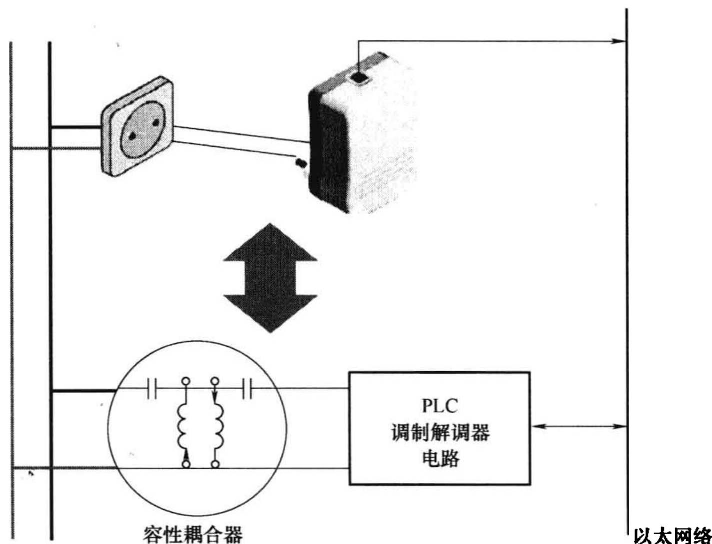


图 7.22　容性耦合的工作原理

耦合

在电场中耦合可以定义为，如何连接磁场中的两个电子回路，使得这两个回路中可以产生电流。由于电容和电感效应，在这两个电子回路之间形成的电场和磁场的作用下，该电流可以在回路之间进行传播。

与容性耦合相比，感性耦合的效率更高。感性耦合使用了两根电力线之间、或者电力线与围绕该电力线的线圈之间的电磁感应作用。与容性耦合器相比，对于某些频率，感性耦合器的信号衰减量要小 10 ~ 15dB。插座与开关盒之间的信号衰减量的范围为 10 ~ 30dB。频率为 15 ~ 20MHz 之间时，该衰减量达到最大值。

注入器是一种连接设备。在 PLC 网络中，可以在建筑物的电气开关柜级使用注入器，直接通过电线周围的电感耦合效应，将某个 PLC 设备连接至电力网络。

图 7.23 所示为 PLC 信号注入器的工作原理。信号注入器由两个元件组成：

1）电磁开口线圈，串绕在电网的中性线上。如第 11 章和第 12 章所述，中性线是将 PLC 信号注入电力网络最有利的电线，因为所有电气设备均不能没有中性线。

2）有线电视调制解调器，通过一根电缆（例如同轴电缆）连接至上面的电磁线圈。

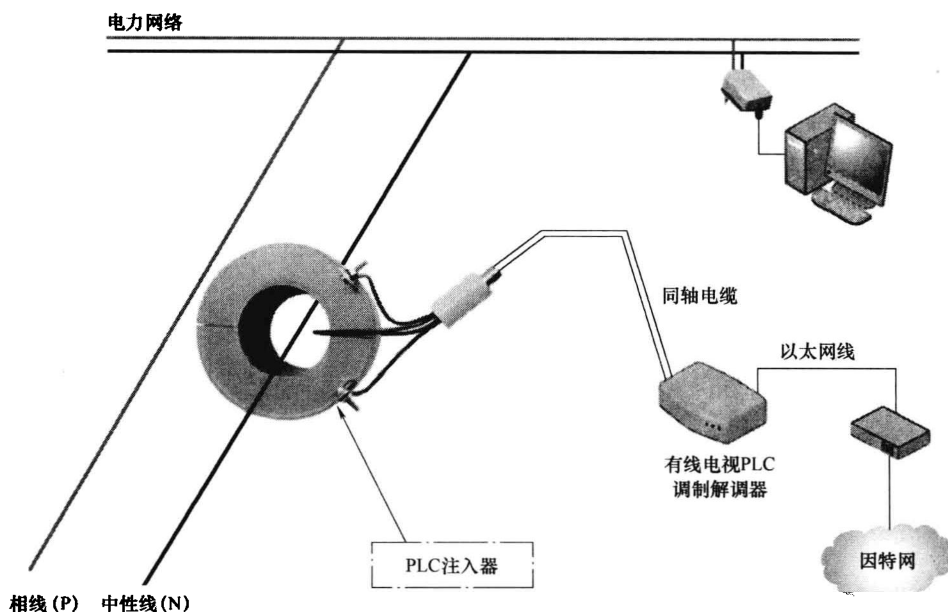


图 7.23 PLC 信号注入连接示意图（使用单相网络上的线圈通过感性耦合方式注入信号）

图 7.24 图示了同一个工作原理，但是，该示例在三相电网上使用两个磁性铁氧体完成信号注入。

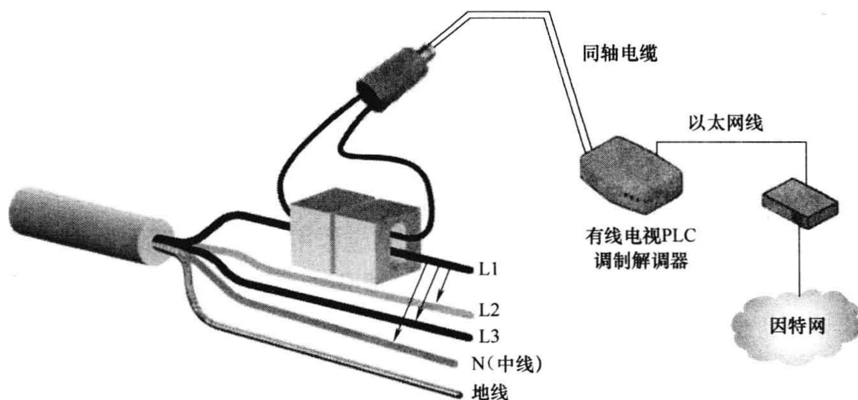


图 7.24 PLC 信号注入连接示意图（使用三相电网上的两个磁性铁氧体以感性耦合注入）

选择注入电缆

将信号注入电力网络时，优先选择将信号注入单相电网的中性线，或者三相电网其中的一根相线。将信号注入单根电缆，与将信号同时注入多根电缆相比，可以获得更好的性能。

使用这种方法连接 PLC 设备，需要操作 110 或 220V/50 或 60Hz 电力网络中的电力线，而容性耦合方法，仅需要将设备连接至某个插座上即可。完成这种耦合操作时，需要很好地掌握接近电网电缆或电网组件时可能存在的电击事故的相关知识，因此，关于这种耦合操作，必须注意合格的专业电气工程人员才可以执行。

图 7.25 为 EichhoffPLC 注入器。该注入器配有开口式电磁线圈（左图）和封闭式电磁线圈（中图），线圈环绕着电力线。这种型号的注入器连接至有线电视调制解调器时，可以使用 F-type 同轴电缆连接器（右图）。

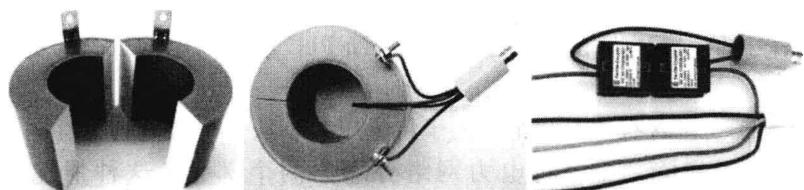


图 7.25 Eichhoff PLC 注入器（带有线圈和磁性铁氧体）

直接抽头法

使用直接抽头法，可以刺穿电缆绝缘层和电力线本身，直接将 PLC 设备连接至电力网络的电力线之上。

由于存在电击危险，该类工作必须由获得授权、可以对低压（LV）或中压（MV）电网电线进行穿刺操作的电工来完成。

图 7.26 为直接抽头耦合方法的工作原理简图。

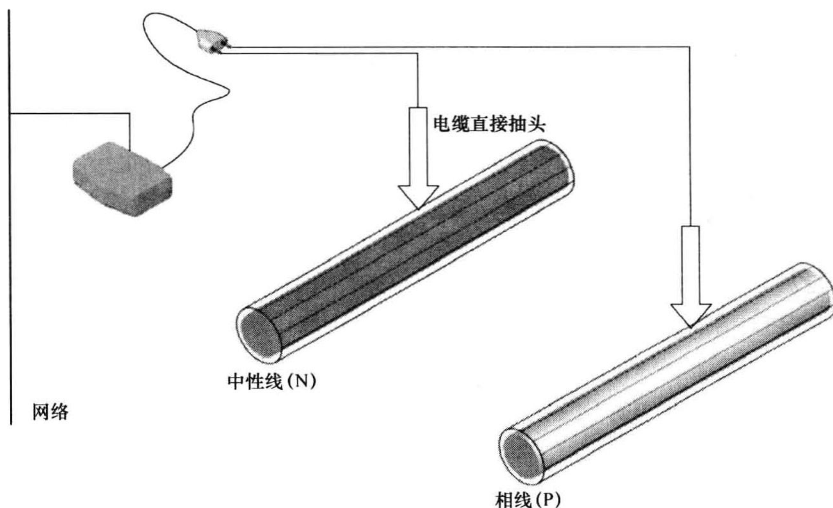


图 7.26 直接抽头耦合方法的工作原理

7.4 变压器和电能表

设计 PLC 网络的拓扑结构时，必须掌握 PLC 信号在电力网络上的传播范围，并确定网络上可能接收这些信号的位置。此外，使用这些信息也可实现 PLC 网络的安全功能。

在安装有 PLC 设备的电力网络上，某些设备对 PLC 网络有影响，且其影响可以达到改变、甚至于完全切断所传输信号的程度。因此，必须在电力网络上不可能切断 PLC 信号的位置注入信号。至于可能切断 PLC 信号的电网设备，我们着重讨论以下设备：

1）变压器（包含有两个绕组，用于将电压大小从一个数值转变为另一个值）。这些绕组可以视作隔离器，将电力网络分隔为两个部分，这种情况称为“电流隔离”。

2）集成了电流隔离装置的某些类型的电能表也可能起到 PLC 信号切断器的作用。不过，这种类型的电能表相对较少，大多数电能表都允许通过 PLC 信号。

这两种情况下，跨越这些设备可能较为有利，因为，这将使得 PLC 信号能够可靠地延伸并覆盖整个电力网络。

7.4.1 变压器

本质上，变压器是一种可靠地物理隔离不同电压的两个电气回路的电气设备，因此，变压器将会阻止 PLC 信号在电力网络这两个部分之间的传输。这种情况下，必须为变压器额外添加某种 PLC 设备。这种设备可以提取变压器某一侧的 PLC 信号，并将重新注入到变压器的另一侧。此外，这种设备还可以放大信号，使得信号足以覆盖整个低压电力网络，直到抵达终端用户的 PLC 调制解调器。

图 7.27 为变压器跨接方法。该方法中，使用了不同的 PLC 信号注入点，且将终端用户的 PLC 调制解调器设置在电能表的后面。

用于跨接变压器的 PLC 设备，其安装方法必须获得电网运营商的批准。这是因为安装该类设备时，必须进入中压/低压变压器房。

7.4.2 电能表

电能表用于测量某个家庭的电能消耗，并可为电力网络用户或者另一个国有电力公司用户开具发票。

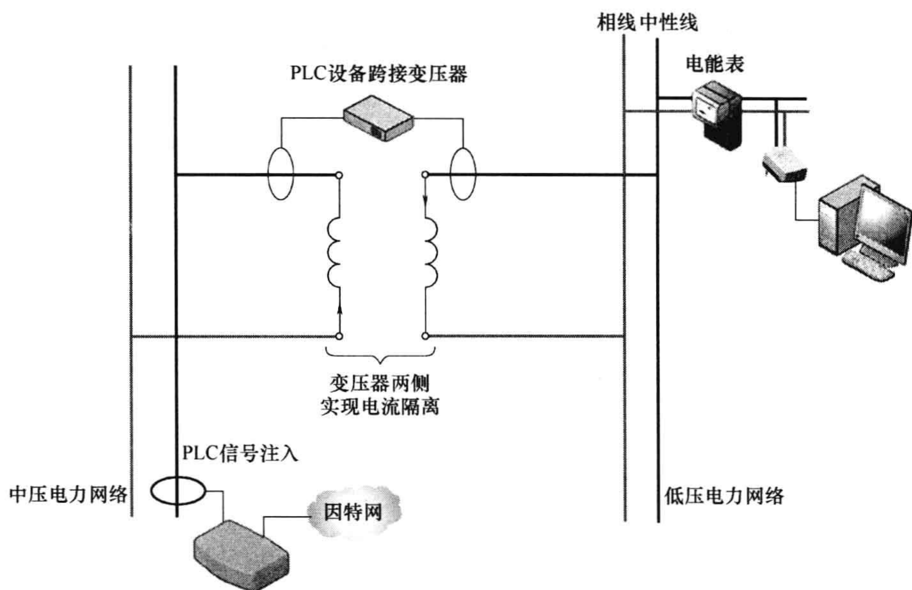


图 7.27 变压器跨接方法

这些组件实现了楼宇、住宅或公司中的供电网络与公共电网的隔离，因此它们是电力网络中关键的 PLC 信号组件。

电能表两侧的电力网络中的 PLC 信号均可以通过大多数电能表。因此，如果希望避免恶意截获电力网络上的数据流，则必须正确、仔细地配置 PLC 局域网上的加密方案。

机电式电能表是历史最久远的一种功率计。这类电能表问世于 20 世纪 70 年代。目前，电能表在电气设备中的使用频率极高。电能表任意一侧电力网络中的 PLC 信号均可以通过这种电能表。它们评估的 PLC 信号的衰减量为 20dB。

为了防止盗窃行为，自 20 世纪 90 年代以来，电子式电能表逐步替代了这种机电式电能表。电子式电能表的抗盗窃能力极强，通过电力网络，借助传输速率极低的低频 PLC 技术，还可以实现远程抄表功能。它们也支持 PLC 信号的发送功能。它们评估的 PLC 信号的衰减量为 15dB。

7.5 中继器

中继器是一种常用电信设备。当传输距离非常远时，使用中继器可以重新生成已接收信号的数据传输信号，使得数据传输设备能够使用这些信号。

在 PLC 网络中，电力网络可能导致 PLC 信号出现衰减现象（原因有信号在电

力网络组件之间的传播、已连接设备的噪声、电力线的质量等)。某些情况下，如果不对信号进行中继处理，这种衰减甚至可能导致网络内两个长距离点之间的 PLC 链路无法工作。

有两种类型的中继器：无源中继器和有源中继器。无源中继器通过使用两个 PLC 芯片，将信号从一个芯片传递至另一个芯片，实现了 PLC 信号的重新生成。中继过程在物理层和 MAC 层完成。有源中继器无需使用另一个 PLC 芯片对信号进行中继，就可以放大电力线上的 PLC 信号。中继仅发生在物理层。

图 7.28 给出了中继器的一种应用示例。

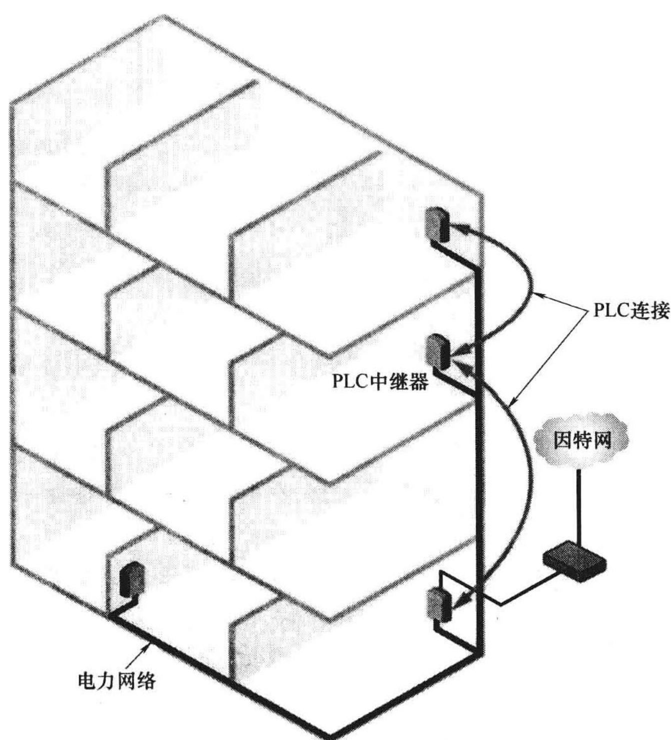


图 7.28 PLC 中继器的应用示例

自从 PLC 设备可以令人满意地传播 PLC 信号之后，已经有几种中继器面市。然而，通过对 PLC 信号的中继处理，在整个电力网络上获得合适的传输速率，更让人感兴趣。

市场上，有如下 PLC 中继器可供选用：

- Schneider IR LR 1100；
- Asoka PL8230-2RP (有源型)；

- Oxance PLT300、PLT320（有源型）；
- CMM RPT1-0。

自制 PLC 中继器

使用市售以太网 PLC 调制解调器，可以自制 PLC 中继器。

自制 PLC 中继器时，仅需使用两个以太网 PLC 调制解调器，采用一根以太网电缆将它们连接起来（使用交叉电缆还是直通电缆，具体取决于网络接口卡是否是自检卡，即网卡是否能适应交叉网线）。此后，必须为各个 PLC 调制解调器配置两个不同的 PLC 网络密钥；调制解调器使用该密钥可以连接至具有相同密码的 PLC 网络部分（见第 10 章）。

图 7.29 展示了这种工作原理。

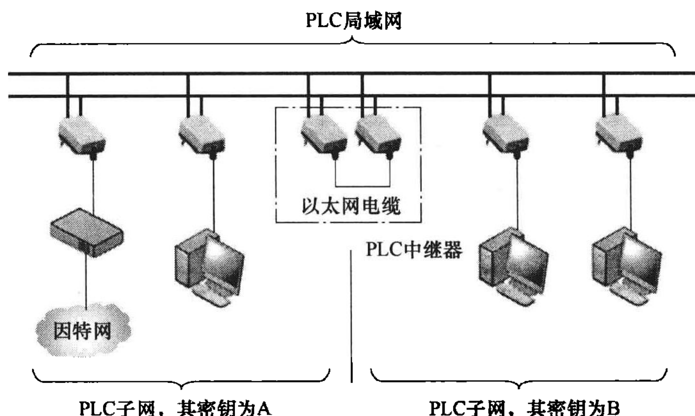


图 7.29　自制 PLC 中继器

两个 PLC 子网通过中继器实现彼此之间的通信。中继器则由两个以太网调制解调器组成，各调制解调器的加密密钥各不相同。然而，在这种配置中，中继器在重新生成 PLC 信号时，需要占用电力网络带宽。因此，这种配置的缺点就是会显著地降低整个 PLC 局域网上的可用数据吞吐量。

7.6　滤波器

如前所述，作为一种通信介质，电力网络会因其所连接的电气设备产生的干扰而被改变。

当电气设备会发回 PLC 设备工作频段内的电磁噪声时尤其如此。因此，将滤波器安装在尽可能接近干扰设备的位置，对于抑制干扰频率越为有利。

也可以使用 PLC 滤波器阻止 PLC 信号意外流出，使得信号传播范围严格限制在电能表分隔的电力网络之内。

图 7.30 所示为一个电力网络示意图，该网络含有 PLC 设备、干扰设备（调光器、吹风机、接线板和断路器等）、PLC 滤波器（对于滤波器，还指出了其安装位置）。

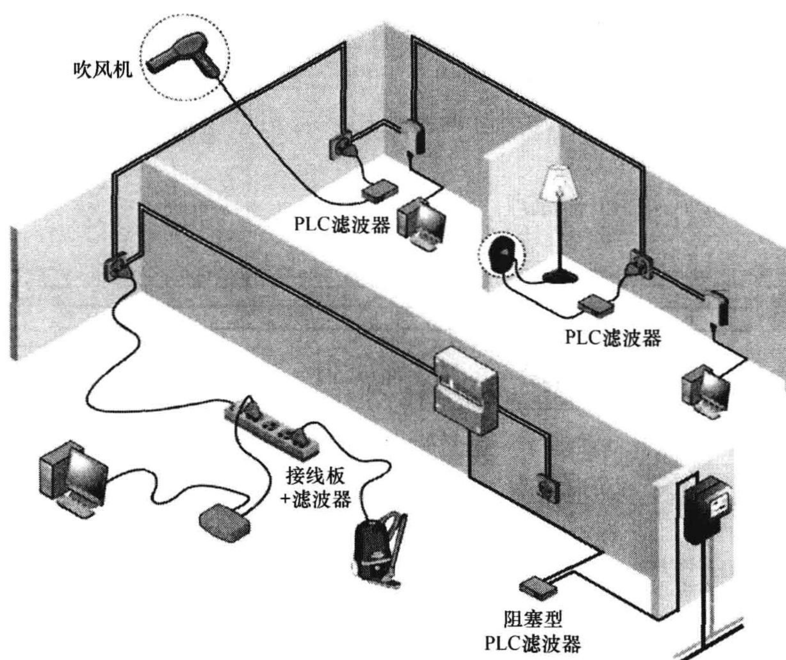


图 7.30 安装在家用电器网络上的 PLC 滤波器

滤波器安装在干扰设备和电力网络之间。滤波器充当了插座之上的上层插座，用于连接干扰性电气设备。

表 7.5 简要列出了对局域网有不良影响的、主要的电气设备。

图 7.31 为 Eichhoff PLC 阻塞式滤波器。该装置安装在电气配电盘和家用、专业与工业电气网络之间，防止 PLC 信号流经电能表，并可以从另一个电力网络恢复该装置。

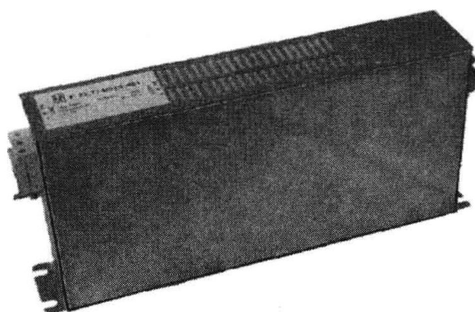


图 7.31 Eichhoff PLC 阻塞式滤波器

表 7.5　对 PLC 网络存在干扰影响的电气设备

电气设备	干扰原因
吹风机	电动机
阴极射线管显示器	阴极射线管
钻床	电动机
调光器	调光和齐纳二级管
卤素灯	调光和齐纳二级管
接线板	电气连接存在缺陷，同一个插座连接了过多设备
未合格通过 CE 标志认证的设备	存在干扰模式以外的干扰

Courant MultiMédia（CMM）公司向市场推出了插座上层抗噪声滤波器。这种滤波器安装在 PLC 网络潜在的干扰设备和可能存在问题的设备的供电插座之间。该设备如图 7.32 所示。

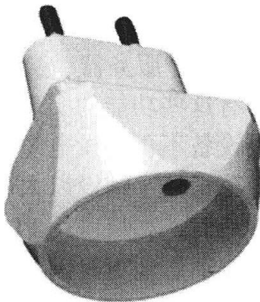


图 7.32　CMM 公司抗噪声 PLC 滤波器

法国的电力线通信公司（LEA 公司）开发了一种全功能型 PLC 滤波器和调制解调器。这种设备通过电源插座使用，可以滤除电源插座上所连接的电气设备所产生的干扰信号。使用这种设备，可以使得电源线免受连接在 LEA 公司的 NetSocket200 + 所连接的多功能插座上的设备的干扰。作为一种整体式全功能滤波器装置，这种装置在 PLC 领域非常独特，它节省了一个电源插座，并可以连接多个电气设备。图 7.33 所示为 LEA 公司的 NetSocket200 + 示意图。

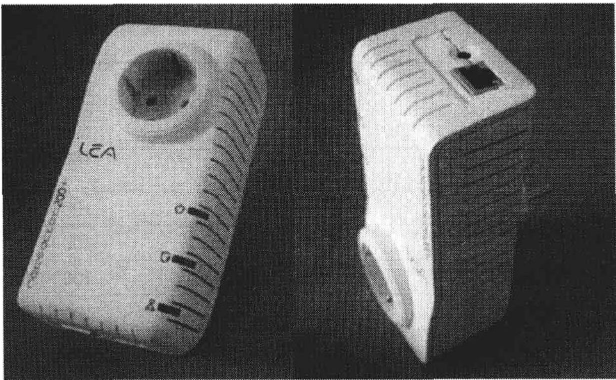


图 7.33　LEA 公司的 NetSocket200 + 示意图

7.7 PLC 的成本

随着 HomePlug 规范和要求的不断提高，2005 年和 2006 年，PLC 产品的价格一直在下跌。2003 年（当年发布了第一台 HomePlug 1.0 产品的技术数据）至 2005 年期间，价格下降的幅度约为 30%。

2006 年初，出现了 HomePlug Turbo 产品，更加加剧了价格下跌的趋势。我们认为，HomePlug 1.0 产品的价格仍然会继续下跌 20% ~50%。

2006 年末，第一种 HomePlug AV 产品面市时，HomePlug Turbo 的价格立即就下跌了 10% ~20%。

对于个人用户来说，PLC 是多 PC 共享同一个因特网连接的一种理想的解决方案。此外，这也是 PLC 设备最常见的应用。今后，PLC 设备，尤其是多功能 PLC 调制解调器，将会整合所有的功能，并可以用作因特网调制解调器、路由器、防火墙、DHCP 服务器、交换机、Wi-Fi 接入设备（即整合了 6 种设备的功能）。考虑到所有这些功能的实现成本，这些 PLC 设备的价格无论怎样都极具吸引力，而且该类设备不再铺设电缆和加工穿线过孔。

公司楼宇铺设以太网电缆时，电缆必须铺设至每一个房间，且必须安装通信柜。然而，如果采用 PLC 技术则无需如此。相对以太网来说，PLC 的另一个优势是可以动态地更改网络拓扑结构。对于以太网，更改网络拓扑常常需要铺设新电缆，并因而需要追加成本。

表 7.6 所示为 2008 年春季季末 PLC 设备的成本简表。

表 7.6 PLC 设备的成本

设　备	成本/欧元
USB 调制解调器 HP 1.0 Turbo	 50 ~ 100 80 ~ 100
以太网调制解调器 HP 1.0 Turbo AV	 50 ~ 100 80 ~ 100 100 ~ 300
有线电视调制解调器	100 ~ 300
集成式插座	100 ~ 300
PLC/Wi-Fi 设备	100 ~ 200
多功能 PLC 设备	100 ~ 300
音频和电话 PLC 设备	100 ~ 150
感应式注入器	120
中继器	200 ~ 400
滤波器	200 ~ 400

第8章 安　　装

安装网络时，必须充分考虑 PLC 网络可能受到和可能导致的干扰。构建 PLC 网络时，安装 PLC 设备的楼宇的电气拓扑也是一个关键的考虑因素。

因此，准确、详细地描述电气网络拓扑是一个必不可少的关键步骤。它对 PLC 网络的数据传输性能起着决定性的作用。无论是移动式，还是安装在电气网络中的固定式 PLC 设备，它们所提供的数据链路质量可能各不相同，并且与它们的位置、附近的干扰信号特性以及用于防止杂散频率信号注入电气网络的滤波器等相关。

由于标称的传输速率与用户所得到的实际传输速率总是不相一致，因此另一个局限性与实际的传输速率有关。意外的传输速率降低与 PLC 系统的某些机制有关。不过，在配置 PLC 设备尤其是 PLC 网关或者关键设备时，如果选用合适的机制和相关参数，就可以将传输速率过低的现象降低至最小程度。

关于安全性，我们发现其关键在于采用合适的技术对数据进行加密并合理地隔离电力网络上的逻辑网络，并且将电力网络视为一个共享的数据总线。由于 PLC 信号的传播会流经家用、专业或者工业设施等的电能表，因此，为 PLC 局域网设置密码以对数据交换进行保护也极为重要。

电气网络的建模极为困难，且其性能会随着所使用的 PLC 设备的改变而快速改变。本章集中描述有助于理解这类改变的相关信息，并讨论如何提高性能。

8.1 频段

常见的公用型和专业型 PLC 使用两个频段：低传输速率时使用的频段为 3 ~ 148kHz；高传输速率时使用的频段为 1 ~ 30MHz 。

中压（MV）电网 PLC 技术也称宽带电力线（BPL），可能使用频段 30 ~ 50MHz。这些技术的安装与实施由中压电网运营商负责。

频段 3 ~ 148 kHz 和 1 ~ 30MHz 被称为豁免授权频段[1]，也就是说该频段的使用既无需授权批准，也无需支付订购费用[2]。不过，这些频段已由 ETSI（欧洲）和

---

[1] 豁免授权频段具体范围根据各个国家的情况不尽相同，请参阅各个国家无线电管理主管部门的规定。——译者注

[2] 使用豁免授权频段的频率根据相关国家的规定可能为免费，但使用该设备可能需要缴纳费用。——译者注

FCC（美国）在发射功率方面制定了某些限制。

这些频段细分为一系列发射用子频段。现在已经发展到所有技术都可以使用这些频段的程度，且标准化工作也在不断向前推进，以至于同一个电气网络上，可以同时存在多个不同的 PLC 系统。在本书第 13 章，我们将会再次讨论 PLC 技术的共存与交互。

8.1.1 无线电频率管理

部署电信网络时，关键的问题是如何在传输速率、时延、时基抖动、电磁兼容性（EMC）和技术共存能力等方面获得最佳性能的同时，确保遵守各种生效的规章所规定的限制。

发射功率和授权频段等方面的规定，均由这些管理规章规定。根据各种无线电技术（业余无线电、模拟短波、数字无线电波等）的不同，这些管理规章还规定了相应的干扰允许水平。

由于相应的技术与传输介质的关系，用于传输信号的电力线设备会因感应效应而发射无线电波。

与 Wi-Fi 无线网络不同的是，欧洲范围内出售的 PLC 设备均尽力遵守欧洲电工技术标准化委员会（CENELEC）和欧洲电信标准协会（ETSI）所设置的限制性规定。实际上，这些设备的设计均遵守这些限制性规定，无论是设备的硬件还是软件，都不允许凌驾于这些标准之上。

HomePlug 设备的软件不得修改任何硬件参数（如载波频率、子频段、发射功率）这意味着，不得使用 PLC 设备配置工具发送的以太网数据帧（见本书第 10 章）来更改设备所使用的频率与功率。因此，对于 PLC 网络用户来说，在配置过程中，不得修改 11 个通道的物理层参数（与 Wi-Fi 不同），也不得对接口传输功率的参数进行修改操作。

图 8.1 给出了配置工具如何给需要配置的 PLC 设备发送以太网数据帧，这种帧是传统的以太网数据帧。在网络上，通过其字段 ETHERTYPE，可以识别这种帧。帧数据中包含有需要配置的参数，由此确保 PLC 网络可以工作于最佳状态。

ETSI 所定义的可用频谱，整体上按照图 8.2 进行了进一步细分。根据监管机构颁发的规定可以看出，一般的公共无线电频率的分布与各种 PLC 技术所使用的频率相当接近。

如前所述，PLC 网络并非无线网络。但是，该技术的实现会在电力线上产生电波辐射，且电力线充当了无线电天线的作用。因此，电信监管机构将 PLC 网络视作无线网络，因此 PLC 网络也必须遵守在发射功率和频段使用等方面的限制。

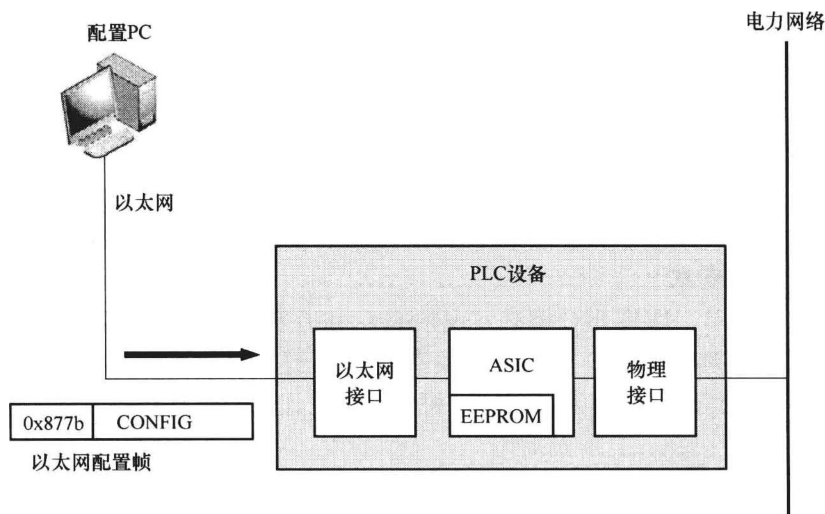


图 8.1 用于配置 HomePlug 网络的以太网数据帧

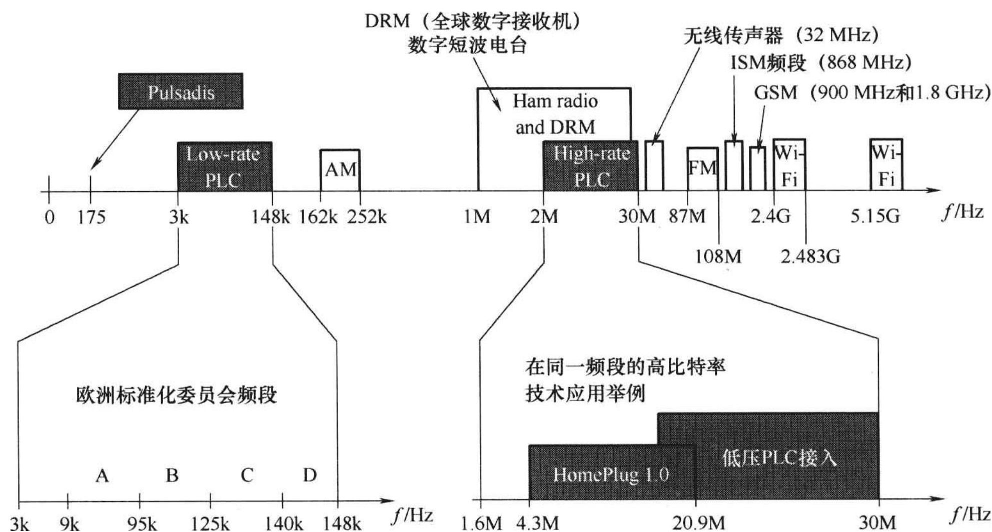


图 8.2 PLC 频段

前面已经指出，高传输速率 PLC 所使用的频率位于 1 ~30MHz 的频段之内。业余无线电台也使用该频段，且今后的数字式短波电台，即 DRM（Digital Radio Mondial）也工作于该频段之内。DRM 将会使用该频段实施超长距离的数字广播节目传输，数据传输速率可达数十 kbit/s。

人们对 PLC 网络对业余电台和 DRM 造成的干扰已经进行了非常多的探讨，以试图使得多种技术可以共存。经过这些讨论，PLC 技术开发商已经在其产品中考虑使用滤波器技术，以避开已经被其他无线电技术使用的频率。这种技术称为“频谱开槽”技术，包含有无线电通道监听来重新调整频率，以及禁用某些频率等技术。

动态频段开槽技术

如图 8.3 所示，如果 PLC 网络发现频率 f_1 和 f_2 已经被使用，则它会禁用它的授权频谱内含有频率 f_1 和 f_2 的频段。频率 f_1 和 f_2 被占用期间，这些频段会一直被禁用。此后，一旦这些频率未被占用，将会再次允许使用这些频段。

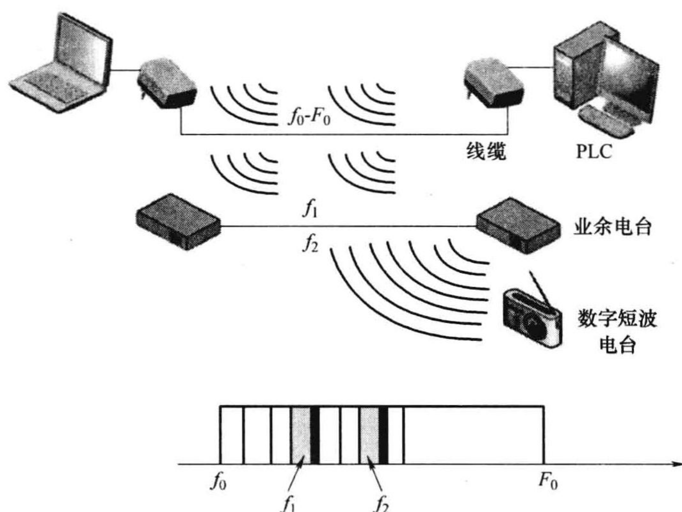


图 8.3 拥挤频率开槽示意图

这种动态技术的基础是信噪比监听技术，每一个频段都会被监听，且信噪比测量值的单位为 dB。

低传输速率 PLC

低传输速率 PLC 主要用于家用自动化设施和汽车自动化功能（机动车辆工业总线），其授权频率由欧洲电工技术标准化委员会在标准 EN-50065-1 中规定。该标准定义了 3～148kHz 之间的所有频段的使用参数。PLC 的信号发射功率以最大允许电压数值来进行规定，对于这些频段来说，最大电压允许值为 3.5V。低传输速率 PLC 频段的参数简述见表 8.1。请注意，调幅无线电台的频段覆盖了 162～252kHz 的频谱。

表 8.1　用于低传输速率 PLC 的 CENELEC 频段

CENELEC 频段	频段/kHz	应　用
	3～9	仅供电气网络运营商专用，例如用于远程抄表
A	9～95	仅供电气网络运营商使用
B	95～125	供家庭自动化使用（婴儿监听电话等）
C	125～140	供家庭自动化使用（X10 等）
D	140～148	供家庭自动化使用

特例：日/夜费制电能表的 EDF Pulsadis 信号（法国）

Pulsadis 信号更为人熟知的名字是日夜信号，原因在于法国的 EDF 电能表使用该信号在夜间切换大量的用电设备，以使得客户受益于 EJP 费率或者 EDP 计时器。该信号在 EDF 供电网络上以 175Hz 的频率发送。

图 8.4 描述了支持 Pulsadis 信号的低压电气网络的电气架构，Pulsadis 信号自 EDF 监控站出发，最终抵达消费者的电能表。

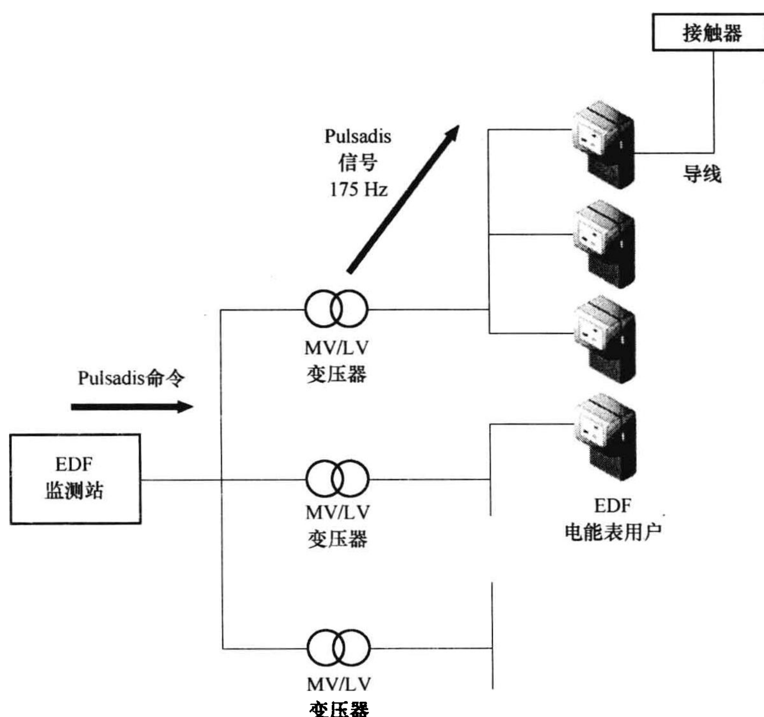


图 8.4　EDF 低压电网上 Pulsadis 信号的实现结构

该信号一旦抵达 EDF 日/夜费制电能表，将立即触发在家用断路器面板上特定安装的电气设备的接触器。例如，该接触器可以在夜间接通热水器的电源，并在早

上7点回到全额费率之前切断热水器。

这种信号是一种低频信号，在电力网络上有着良好的传播性能。其频率为175Hz，避开了50Hz及其相应的谐波频率（100Hz、300Hz、600Hz等）。该信号由间隔1.5s的时长为1s的二进制脉冲构成。帧长为102.25s。

高传输速率 PLC

高传输速率PLC或多或少地使用了1～30MHz频段。通常，该频段可以视为两个子频段：1～20MHz的较低频段和2～30MHz[⊖]的较高频段。前者专门用于家庭内部PLC；后者专门保留，供中压电力网络的公用外部PLC使用。

涉及家用内部PLC时，各种不同技术均基于正交频分复用（OFDM）技术，且这些技术可以以不同方式共享频段，以在传输速率和时延等方面达到最好的性能。这种性能的获得是通过不断改进物理层（PHY）、数据链路层和MAC层等的调制技术以及物理介质访问方法而实现的。

HomePlug 1.0使用了4.49～20.7MHz的频段和84个子载波，将0～25MHz的频段细分为128个宽为1953125kHz的子频段。据此，如果将各子频段依次编号为1～128，则HomePlug1.0使用了子频段23～106。

在美国，业余无线电者使用了子频段23～106中的某些频段（17m、20m、30m、40m）。因此，没有使用与业余无线电频率相对应的8个子频段。因此，HomePlug 1.0频段的总数量为84－8＝76个。

表8.2按照各种PLC技术简要地列出了可以使用的高传输速率频段。

由于频段1～30MHz被细分为多个子频段，故各子频段传输信道传送的均是OFDM的调制载波。严格地说，与Wi-Fi不同，该技术不存信道用于配置网络架构。在PLC中，整个频段全部用作传输通道；所有的子频段均是为了提高传输可靠性。

表8.2 高传输速率PLC技术所使用的频段

PLC技术	频段/MHz	OFDM载波数量
HomePlug 1.0	4.49～20.7	76
HomePlug 1.1	4.49～20.7	76
HomePlug AV	2～28	917
DS2 45Mbit/s 200Mbit/s	1.6～30 2.46～11.725 13.8～22.8	100 1280＋1280
Spidcom	2～30 30～60（外部）	900 900
Main. net	4.3～13	不连续

⊖ 这里应为20～30MHz，原书可能打印错误。——译者注

此外，与 Wi-Fi 不同的是，配置网络时，无需根据其他已经被分配的通道进行任何选择工作。允许用频段的所有通道，即使用全部所谓的“子频段”。因此，同一电力网络上可以同时使用多种技术，并可能导致网络阻塞。出现这种情况时，PLC 技术将使用空闲或者非常用型子频段。第 13 章中，我们将会讨论 PLC 技术的共存以及互操作性标准的工作进展。

图 8.5 描述了 HomePlug 1.0 PLC 网络中各种 PLC 调制 OFDM 子频段的频率范围和相关的二进制数据。

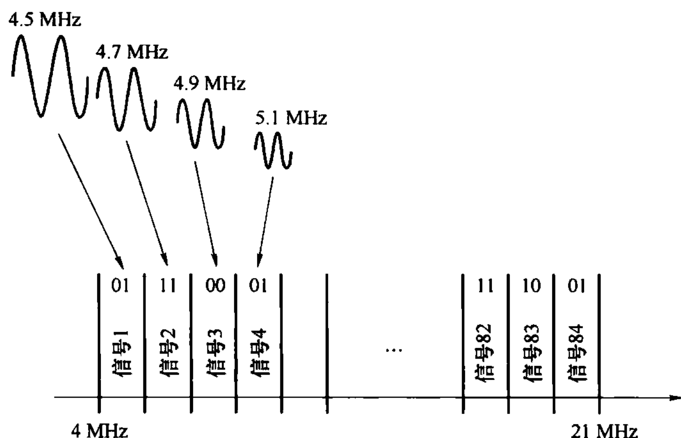


图 8.5　HomePlug 1.0 PLC OFDM 子频段

8.1.2　电磁兼容性和频段

各种家用型、专业型或者工业型电气与电子设备，工作时都会向邻近区域发射无线电磁波。

这些无线电磁设备的频率可能干扰网络中 PLC 设备的正常工作，且妨碍子频段内的数据通信。与 PLC 网络上的其他设备相比，某些设备产生的干扰影响更加严重。例如，欧洲实行的 CE 标志对商用电气与电子设备的无线电磁波辐射进行了强行限制。

第 7 章（见表 7.5）列出了对 PLC 网络存在干扰影响的设备。我们将在本章对干扰进行更加深入的讨论。

与此相反，PLC 设备发射的电磁波也可能干扰电力线周边电信设备的正常工作。国际电工委员会（IEC）的国际无线电干扰特别委员会（CISPR）规定了 PLC 设备无线电波辐射的限制。

目前的 PLC 技术，例如 HomePlug AV，为了符合这些辐射限制规定，采用了

频谱开槽技术。

图 8.6 表明，传输通道可以视作带有子载波的 N 个子频段，所有子频段都可以同时工作，且每一个子频段均传输部分物理层数据。

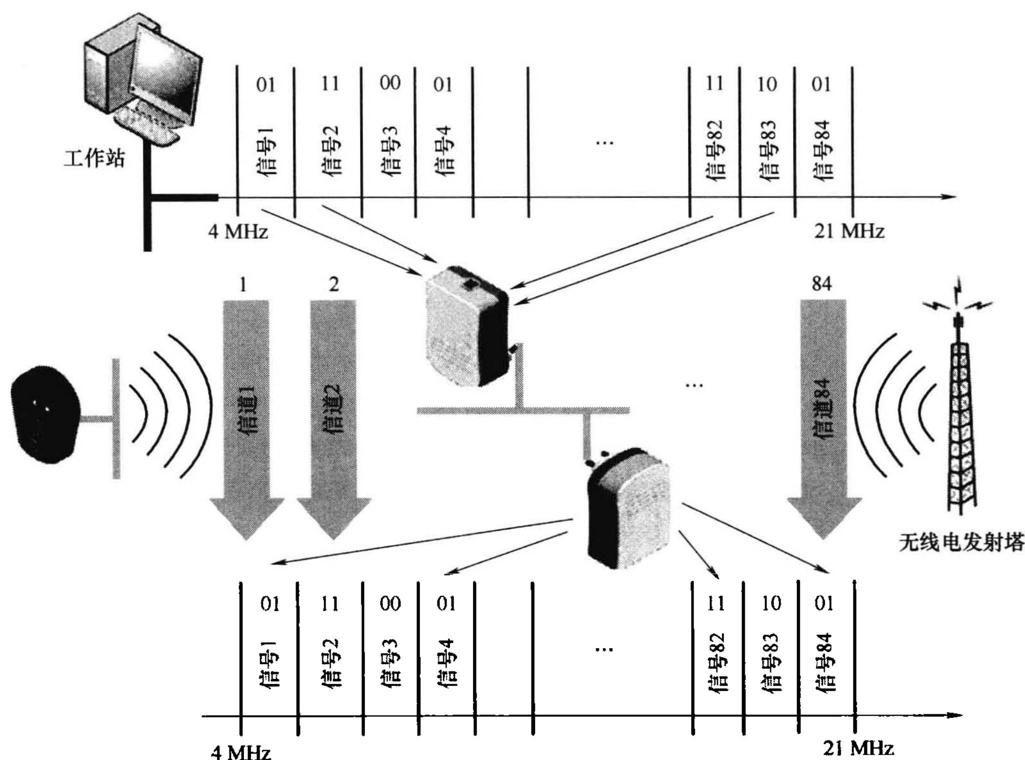


图 8.6 PLC 多通道 OFDM 调制

PLC 设备的传输功率

商用 PLC 设备的信号发射功率，经实测通常为 20dBm（测量使用频段为 1 ~ 30MHz）。该功率可以使用变量 P 或者 G 表示

$$P = 10^{G/10}$$

也就是

$$G = 10\lg P$$

式中，G 相当于增益⊖，单位为 dBm 或 dBi；P 表示功率，单位为 mW。

表 8.3 给出了增益与功率之间的关系。

⊖ 这里的增益是指相对数值的意思，也就是 dBm 数值，是绝对数值的 dB 化。——译者注

表 8.3　增益与功率的对应关系

增益/dBm	功率/mW
3	2
5	3.1
7	5
9	8
15	31.6
19	79.4
24	251.1

对于电力网络中的 PLC 设备来说，其功率极限值为 100mW（也就是频段为 1～30MHz 时，20dBm）。传输通道的性能取决于信号范围。

为了符合 CISPR 根据电磁兼容性（EMC）的规定，必须限制 PLC 设备的发射功率。

测量传输功率时，使用准峰值，而不使用平均值。在该频率范围之内，准峰值对应功率谱密度（PSD），即总发射功率在频段 1～30MHz 的所有子频段上均匀分布。

HomePlug 1.0 技术包含有 84 个宽为 195.31kHz 的子频段，而 HomePlug AV 则包含了 918 个宽度更窄（即 24.414kHz）的子频段。因此，HomePlug AV 的 PSD 波较小，对于物理层协议数据单元的数据传输功率来说，有可能增大 2.2dB。

图 8.7 描述了 HomePlug1.0 和 AV 之间的功率谱密度差。功率谱密度的描述单

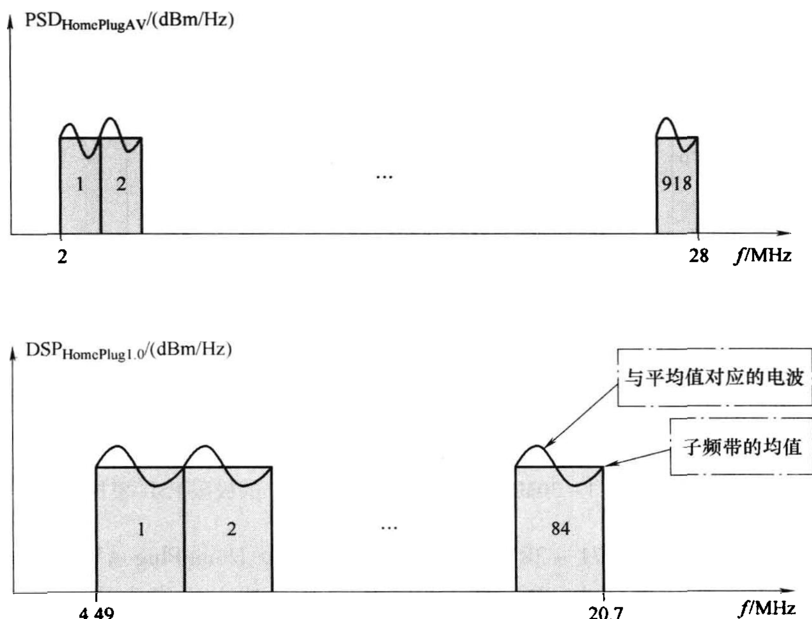


图 8.7　HomePlug 1.0（上）和 HomePlug AV（下）之间的功率谱密度差

位为 dBm/Hz。表 8.4 简要列出了这两种版本中各种不同成分的 HomePlug 物理帧的平均传输功率。

为了符合电磁（EM）辐射限制，HomePlug 1.0 和 AV 的规范规定 PLC 设备的功率谱密度必须小于或等于 -50dBm/Hz。

表 8.4 各个子频率内的传输功率

物理帧组成部分	平均传输功率/dB	
	HomePlug 1.0	HomePlug AV
帧前导	3	3
帧控制（FC）	0	3
物理层协议数据单元中的数据	0	2.2
优先解析符（PRS）	3	3

图 8.8 为频段 1～30MHz 之内的 HomePlug AV 的功率谱密度曲线。从中可以清楚地看出，相对于其他频率，某些频率辐射功能较低（为 -80dB，对应着 50Hz 左右）。可以认为，电力网络和电力线附近的设备对于功率谱密度为 -80dB 左右的那些频率不敏感。

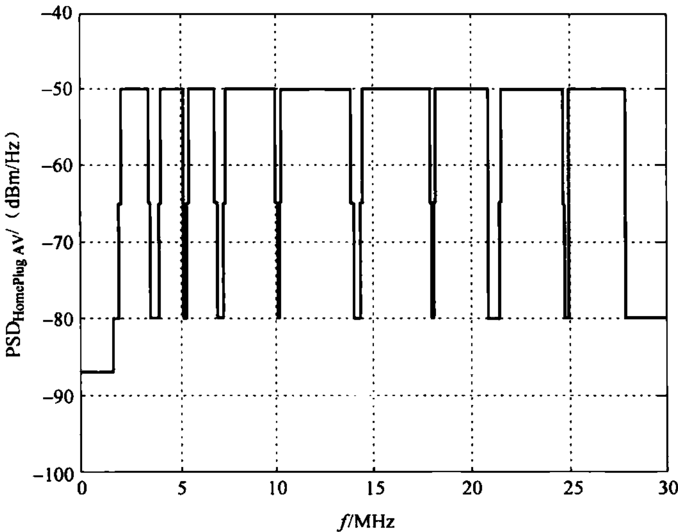


图 8.8 频段 1～30MHz 之内的 HomePlug AV 的极限 PSD 模板

表 8.5 简要列出了 1.71～28MHz 的范围内的各个 HomePlug AV 子频段、各子频段的功率谱密度（单位为 dBm/Hz），以及（其他技术已经占用了某个子频率时）是否启用子频段等信息（这些子频段的编号为 0～1535）。表中最后一列为相

应子频段所对应的无线电技术。

表8.5　各个 HomePlug AV 子频段内的 PSD 和相应的规定

子带 主频率/MHz	最大 PSD /(dBm/Hz)	载波开/关	说　明
$F \leq 1.71$		载波 0~70 关闭	AM 广播频段及 AN 广播频段以下频段
$1.71 < F < 1.8$	-80	载波 71~73 关闭	AM 广播频段和 160m 业余频段之间
$1.8 \leq F \leq 2$	-80	载波 74~85 关闭	160m 业余频段
$2 < F < 3.5$	-50	载波 86~139 打开	HomePlug 载波
$3.5 \leq F \leq 4$	-80	载波 140~167 关闭	80m 业余频段
$4 < F < 5.33$	-50	载波 168~214 打开	HomePlug 载波
$5.33 \leq F \leq 5.407$	-80	载波 215~225 关闭	5MHz 业余频段
$5.407 < F < 7$	-50	载波 226~282 打开	HomePlug 载波
$7 \leq F \leq 7.3$	-80	载波 283~302 关闭	40m 业余频段
$7.3 < F < 10.10$	-50	载波 303~409 打开	HomePlug 载波
$10.10 \leq F \leq 10.15$	-80	载波 410~419 关闭	30m 业余频段
$10.15 < F < 14$	-50	载波 420~569 打开	HomePlug 载波
$14 \leq F \leq 14.35$	-80	载波 570~591 关闭	20m 业余频段
$14.35 < F < 18.068$	-50	载波 592~736 打开	HomePlug 载波
$18.068 \leq F \leq 18.168$	-80	载波 737~748 关闭	17m 业余频段
$18.168 < F < 21$	-50	载波 749~856 打开	HomePlug 载波
$21 \leq F \leq 21.45$	-80	载波 857~882 关闭	15m 业余频段
$21.45 < F < 24.89$	-50	载波 883~1015 打开	HomePlug 载波
$24.89 \leq F \leq 24.99$	-80	载波 1016~1027 关闭	12m 业余频段
$24.99 < F < 28$	-50	载波 1028~1143 打开	HomePlug 载波
$F \geq 28$	-80	载波 1144~1535 关闭	10m 业余频段

8.2　电网拓扑结构

所有楼宇，无论是家用、专业还是工业楼宇，其电力网络布线类型均有两种：

1）单相，仅有两根电缆（中性线和相线）。两根电缆之间的电压为 110V 或 220V。该电压从断路器控制面板流至各个插座，并为楼宇提供照明用电。

2）三相，有四根电缆（中性线和三根相线）。中性线与相线之间的电压为 110V 或 220V；任意两根相线之间的电压差为 190V 或 380V。

相对于单相电网来说，三相电网的传输功率更大，可以为楼宇内的更多电气设

备提供电源，因此某些楼宇更加偏向于使用三相电网，而不是单相电网。三相网络也用于为工作时需要三相电压的电机供电。后续章节中，将进一步详细描述这两种拓扑结构。

8.2.1 单相连接

大多数住宅（公寓、家庭房屋、小型楼宇）均采用单相接线系统，因为，它们的电力供电需求常常在60A以下。

如图8.9所示，单相接线系统包含多根电缆（总线-汇流连接）。这些电缆从断路器面板出发，为家用电器设备和灯泡等提供电源。

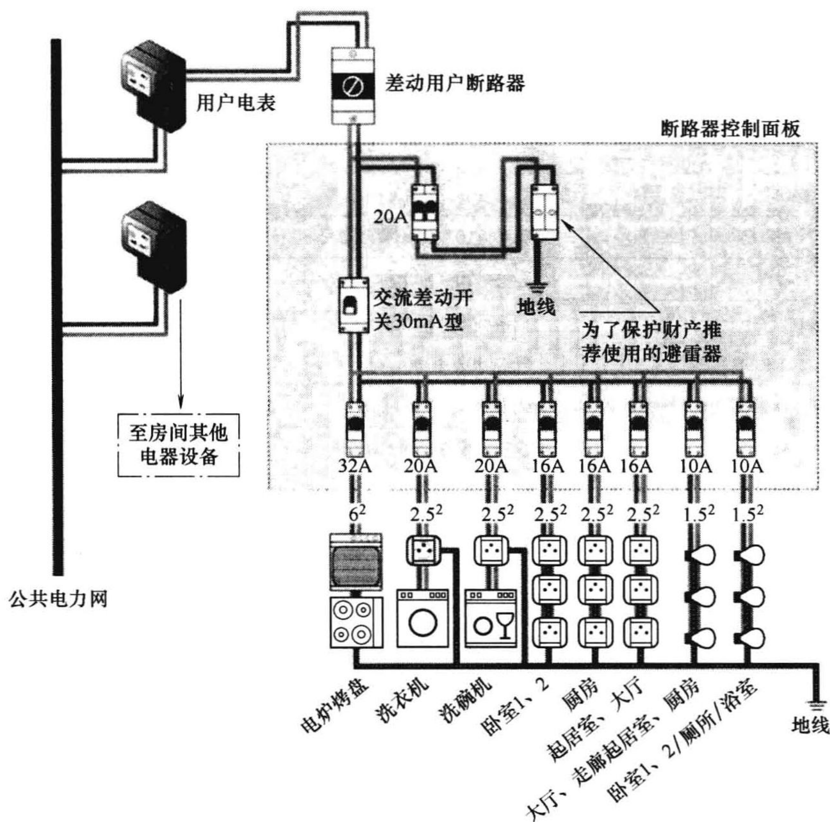


图8.9 家用单相电网的拓扑结构

图8.10为某个公寓单相电网拓扑结构示意图。从中可以看出，各根电缆均从断路器面板接出。PLC设备和调制解调器连接至房间内的插座之上。PLC信号顺着电缆传播，抵达断路器面板，并重新在各个电缆再次开始传播。

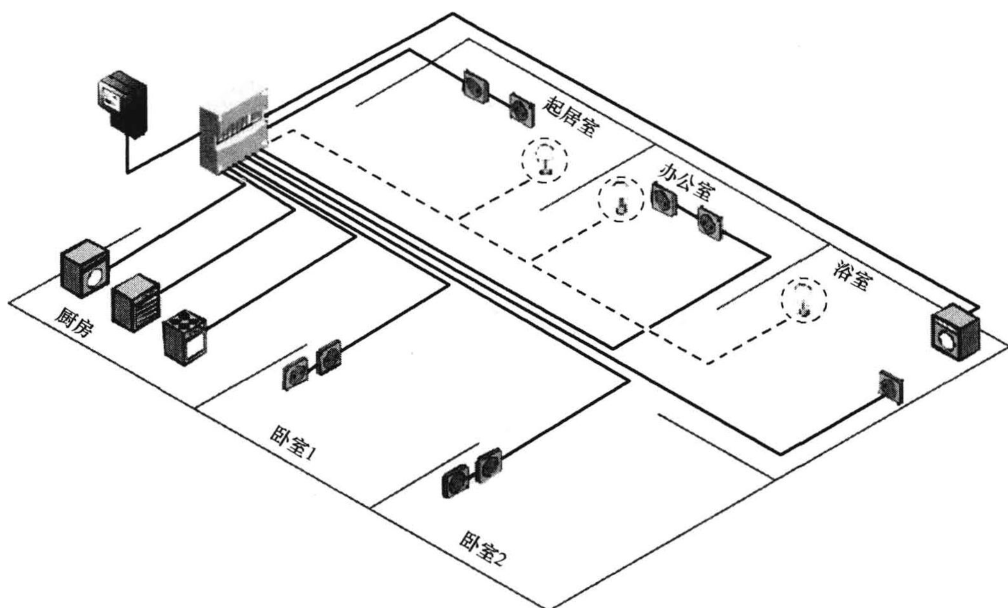


图8.10 公寓单相电网拓扑结构

考虑满意的有用数据吞吐量，可接受的电线布线长度可以达到300m。

该网络上连接的电气设备，对于PLC信号来说是潜在的电磁干扰源。必须牢记，电气控制柜与最远的插座之间的布线长度平均值不得超过200m。

8.2.2 三相连接

楼宇、大型住宅、专业处所或者工厂，对电力的需求量比家用住宅更大，因此，它们的电力网络通常使用三相网络。

三相网络中，从断路器面板接出4根电缆（中性线、相线1、2和3），并为楼宇插座供电。图8.11为楼宇三相接线系统示例。该楼宇为多层结构，且使用不同电力相线为楼宇各层供电。从电气控制柜出发，均有两根电缆连接至各个楼宇层：一根相线和一根中性线。

整个楼宇内，有一根电缆是共用的，即中性线。其他电缆，则在电气上实现了隔离。必须注意，由于存在感应效应，任意一根电缆（中性线或者相线）上流动的PLC信号均可能传输至其他电缆。因此，通过对电力布线属性的优化利用，可以构建PLC局域网的拓扑。

与单相网络类似，断路器面板与最后（远）一个所连接的插座之间的电力布线距离不得超过200m。PLC信号在这些电缆上流动时，如果流经断路器面板之后，再次在其他电缆上传播，则该距离可以超过200m，但是其有用数据吞吐量可能下降。

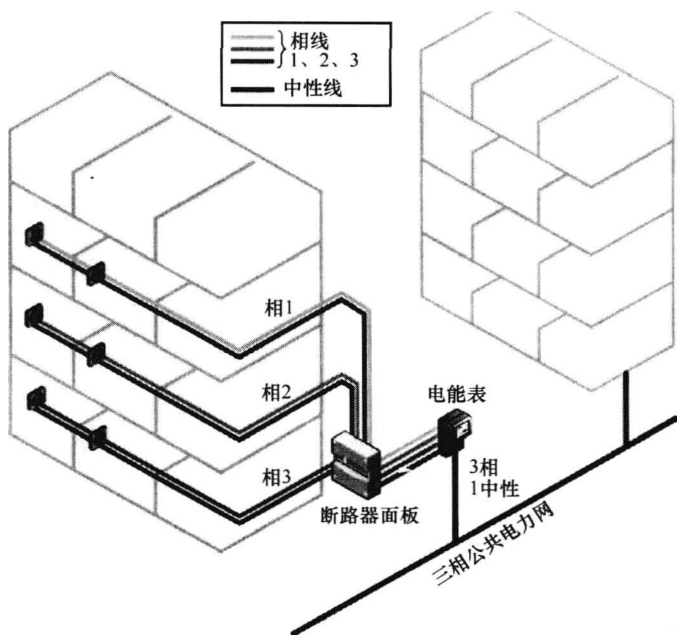


图 8.11 大型楼宇三相电力网络拓扑结构示意图

PLC 信号也可能穿过电能表，并进入邻近楼宇的电力网络。如果需要在楼宇之间构建一个 PLC 局域网，则该特性极为有利。然而，这需要对 PLC 信号进行良好的安全处理，以防止恶意监听 PLC 网络。

8.2.3 电力网络的布线

电缆的横截面积可能影响信号的传播。简单地说，电缆的横截面积越大，信号衰减程度越大。

表 8.6 简要列出了电表与断路器面板之间所使用各种电缆横截面积。

表 8.7 根据电缆上所连接设备的功能（NFC 15-100 标准），列出了相应导线横截面积的推荐值。据此可知，所使用的电缆横截面积主要有 1.5mm^2 或者 2.5mm^2。

表 8.6 EDF 连接电缆的横截面积（取决于传输功率）

进户开关额定电流/A	铜导体最小截面积/mm^2
45	10
60	16
90	25

表 8.7 电气设备所确定的导电电缆横截面积

功 能	铜导线（Ph，N，T）的横截面积/mm²	
标准	NFC 15-100 标准	
照明和控制开关	8	1.5
插座	8	2.5
洗衣机	1	2.5
电炉（平板烧烤炉）或者整板	1	6
单独的烤箱	1	2.5
双头炉灶（室内型）	1	2.5
储水式电热水器	1	2.5
加热：对流式加热器、板式取暖器	5	1.5（最小值）

8.2.4 断路器面板

断路器面板是电力网络的核心设备，所有电力布线均从该设备开始。该面板也是防止电击危险的关键组件。

保护装置采用了所谓的“断路器”（在早期网络中也使用熔丝）。断路器有多种类型。对于PLC信号在电缆上的传输衰减来说，每一种断路器的具体特性各有不同。

图8.12所示为封闭型（左图）和开放型（中图）断路器面板的示意图及断路器面板的前视图（右图）。面板对其所连接的设备进行了标示。

8.2.5 电力网络的衰减作用

我们已经知道，直线距离超过300m（电缆卷绕时，因自感效应，该长度会有所不同）时，由于信号衰减，有用数据吞吐量会急剧下降，以至于无法为上层应用提供满意的服务质量。

由于各电缆的横截面积和阻抗特性各不相同，因此，对PLC信号的衰减作用也各不相同。长度为100m且用于低压公共电网时，HNS33S33电缆对频率为30MHz的PLC信号的衰减量为14dB。

楼宇内的低压（LV）设施可以使用多种类型的电力布线。

1）用于导线、相线、中性线和接地线等的电缆均使用墙内走线，也可以使用彼此独立的电缆护套，但是，这些电缆不得成组使用同一个护套。这种布线类型将电缆布置在彼此非常邻近的环境之内，因此，具有较高的电磁辐射。由于这类电磁辐射的能量损失，PLC信号在这些电缆上的传播会受到非常大的衰减作用。H07 V-U或H07 V-R（刚性导体）、H07 V-K（柔性导体）、P/N采用导管、装饰条或者墙脚等方式走线的设施内，通常使用这些电缆。

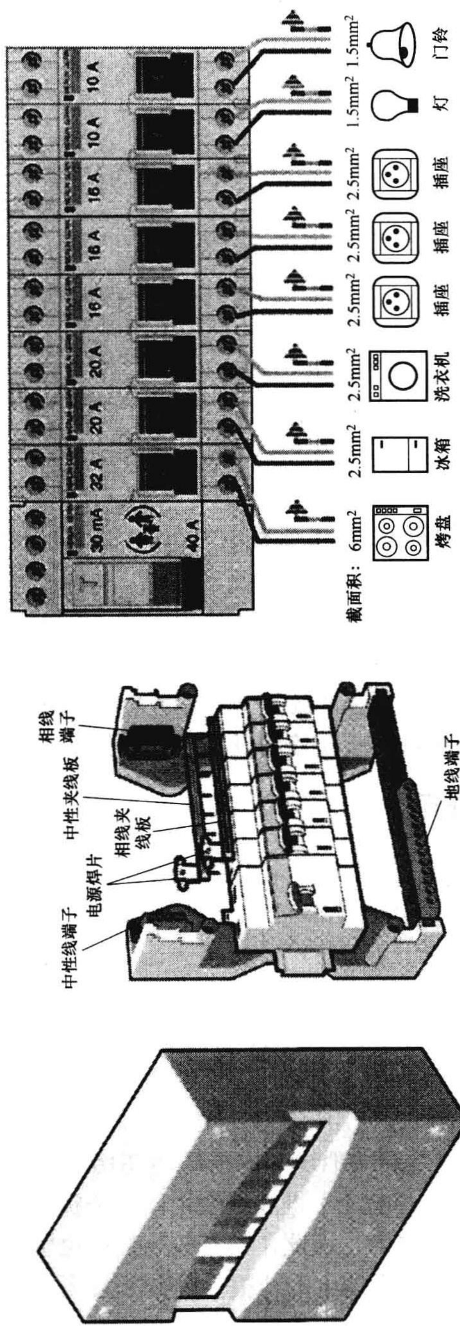


图 8.12 室内安装型断路器面板

2）电缆P、N和G使用绞合在一起的方式安装，且接地电缆编排在电缆护套内绞合线的中间。使用这种电缆安装方式时，电缆之间彼此存在电磁耦合效应，因此PLC信号的传播效果较好。此外，类似于电话线，这种绞合方式对PLC信号具有更好的导向作用，避免了在拥挤的环境因电磁泄漏而导致的衰减现象。这种情况下，信号会相对可靠地约束在电缆护套之内，无论从传输距离还是从传输速率来看，均可以达到更佳的性能。FR-N 05 VV-U或R（刚性电缆）、A05 VV-F或H07 RNF（柔性电缆）P/N采用表面安装、架空安装、导管安装、装饰条安装或者墙脚安装等方式的设施内，通常使用这些电缆。

3）在放入电缆槽或者楼宇墙体内之前，则电气安装师将电缆P、N和G绞合在一起。这种布线类型可良好地传播PLC信号，且电磁辐射导致的辐射损失极小。

常见室内安装的推荐电缆长度

对于普通的住房（即100m² F4单层住房或者65m² T3-T4公寓），断路器面板与插座之间的电缆长度通常为15m。

断路器面板与最远的用电位置（照明地点或者插座）之间的最大电缆长度通常为50m。必须将电缆的线压降控制在2%，以确保连接至设施网络上的电气设备所获得的电压在允许值范围之内。

对于单相电缆，可以使用下式来确定相应的电缆长度，即

$$L=\Delta_u\frac{U_0}{100}\frac{1}{2\rho}\frac{S}{I}\text{ m}$$

式中，Δ_u为以百分比表示的电压降；U_0为电力网络的电压值（110V或230V）；ρ为电力线的电阻率（对于铜导线为0.023，对于铝导线为0.037）；S为电缆横截面积，单位为mm²；I为电缆内流通的电流强度，单位为A。

对于电压降为2%的铜电缆，上式变为

$$L=100\times\frac{S}{I}\text{ m}$$

对于横截面积为1.5mm²、最大允许电流为16A的照明用电缆，建议电缆长度不要超过9.3m。对于横截面积为2.5mm²、最大允许电流为20A的插座供电电缆，建议电缆长度不要超过12.5m。

8.2.6 选择PLC网络拓扑

PLC局域网必须与楼宇内的电力网络相适应。每一个楼宇均可能使用不同类型的电缆、断路器面板、断路器、切断开关（熔丝、断路器），且各回路组件可能使用串联（插座以串联方式连接至电力线）也可能使用并联（插座电缆直接连接至断路器面板）连接方式。

与 Wi-Fi 网络必须适应楼宇墙体结构以避免无线电波的传播障碍类似，PLC 网络也必须与电力网络和电缆槽相适应，以避免在 PLC 信号传播过程中可能存在的障碍。

PLC 局域网的拓扑结构与电力网络的拓扑结构之间的适应可以采用以下一种或多种方式：

1）尽最大可能确定出电力网络的拓扑结构，例如通过电力网络接线图的获得或者通过对楼宇各个插座的 PLC 测试。

2）寻找 PLC 设备接入电力网络的最佳连接点，以获得最佳的 PLC 覆盖率。由于所有的电力布线都源自断路器面板，因此，断路器面板是电力网络的中心点。

3）对于 PLC 信号未能覆盖的电力网络区域且已经连接至其他电力网络的楼宇部分进行标示；对各个插座进行考察，以查明电缆长度是否超限或者是否存在过多的干扰。

在第 11 章和第 12 章，我们将会再次仔细地讨论拓扑结构的选择问题。

8.3 PLC 信号的传播

在 PLC 技术中，其中的一个一再重复的问题是信号在电力线上的传播。这些导线都具有特定的阻抗，会对信号传播产生与电缆长度成正比的衰减作用。

PLC 设备制造商和电信测试实验室的测试结果、PLC 网络的部署反馈信息等，都可以用来修正与 PLC 信号传播有关的某些计算值。

“内部”电缆指私有电气网络（即室内、专业或者工业楼宇内的电气网络）所使用的电缆。对于直径为 1.5mm 和 2.5mm 的铜电缆，可以采用多种测量方法，根据电缆长度，对其信号衰减进行评估。

图 8.13 给出了在 3 个主要频率上进行的此类测试的结果：10MHz、20MHz 和 30MHz。我们注意到，在频段 1 ~ 30MHz 之内，频率越高，衰减程度越大。对于室内安装，电缆长度的平均值为 200m，由于这些设备所使用的接口具有足够的信号接收灵敏度，因此，这种情况下的 PLC 信号衰减量还是足可保证数据传输的可靠性。

“外部”电缆指用于公用设施的公共电网之内的电缆。

这些电缆均是三相低压或者中压电缆，可以是敷埋型也可以是架空型。敷埋型电缆对电磁干扰相对不敏感，而架空电缆对电磁干扰的敏感程度则大得多。但是，还是远远小于内部电缆对电磁干扰的敏感程度。内部电缆因邻近家用设备而承受非常严重的干扰。

表 8.8 简要地列出了不同 PLC 技术可以获得的性能。

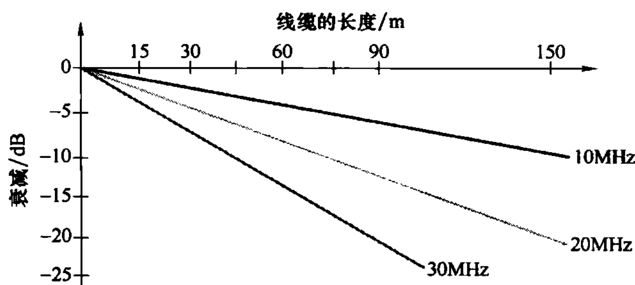


图8.13 PLC信号衰减量与电缆长度之间的关系

表8.8 PLC信号在外部电缆上的传播距离

PLC技术	电缆类型	距离/m	TCP传输速率/(Mbit/s)
Oxance HomePlug Turbo (1.1)	敷埋型	1300	3
Spidcom	敷埋型	3000	3

8.4 干扰

干扰这一概念对于PLC网络极为重要。PLC在电力线上传播时，会在电缆周边辐射频段为1～30MHz的电磁信号，且连接在电力网络上的设备也会对PLC信号本身带来干扰。

此外，对于两个PLC工作站之间的链路来说，两个方向的通信也不可避免地存在特性不一致的现象。通信介质的物理特性（阻抗、电荷、电容）也可能因信号传播方向的改变而改变。

对于工作在电力网络上的PLC设备，各个国家的，或欧盟的以及国际的标准机构均颁布了相应的法规，试图限制这些PLC设备的电磁辐射。如第1章所述，这些设备的电磁辐射必须控制在某个已经设定的最大准峰值之内。IEC CISPR 22修正案已经将功率谱密度（PSD）的临界值规定为-50dBm/Hz。

干扰对电力网络的影响作用

电网插座所连接的电气设备对PLC网络有着干扰作用和电磁干扰。

图8.14给出了对PLC局域网有影响作用的干扰源。

电气设备在启动和工作期间，会产生各种噪声（广谱噪声、脉冲噪声、高斯噪声等）。这些噪声均一化后，相当于覆盖1～30MHz的整个频段、幅值为30dBìV/m的噪声。产生这些噪声的设备过多，难以一一列出，但是，已经确定可能成为噪声源的设备有等离子显示器、卤素灯、真空吸尘器、调光器、微波炉、电视机、计算机显示器、空调、加热器等。

图8.15根据日工作时间，使用在大量家用电器上进行的各种测量的平均值，

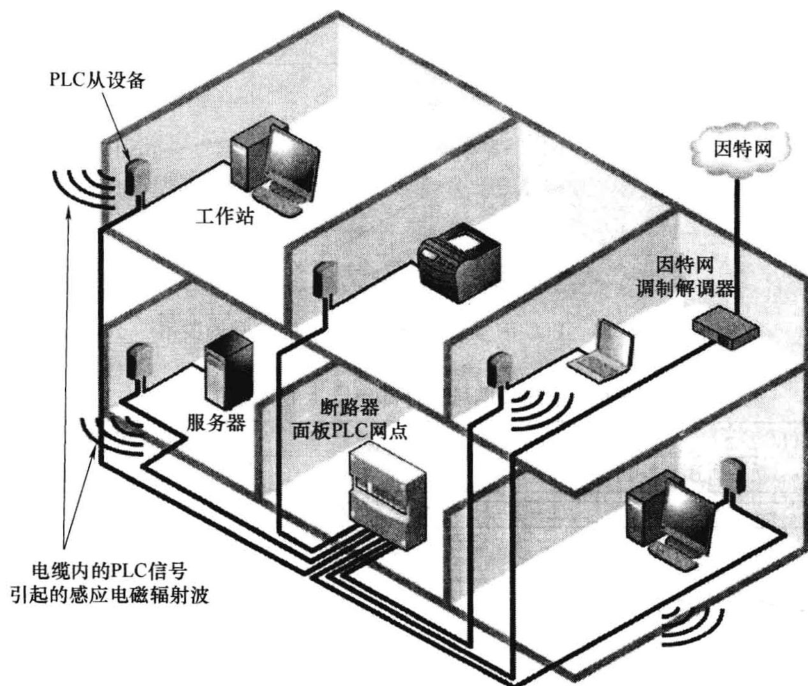


图 8.14 连接到电力网络上的 PLC 设备导致的电磁干扰

给出了电气设备的各种干扰曲线。每一天的结束时段，电气网络上的大量设备会同时工作，从而会存在程度较大的干扰。从图中可见，干扰信号的幅值随着频率的改变而改变。其中，在 10MHz 和 20MHz 附近，存在两个相应的幅值峰值点。

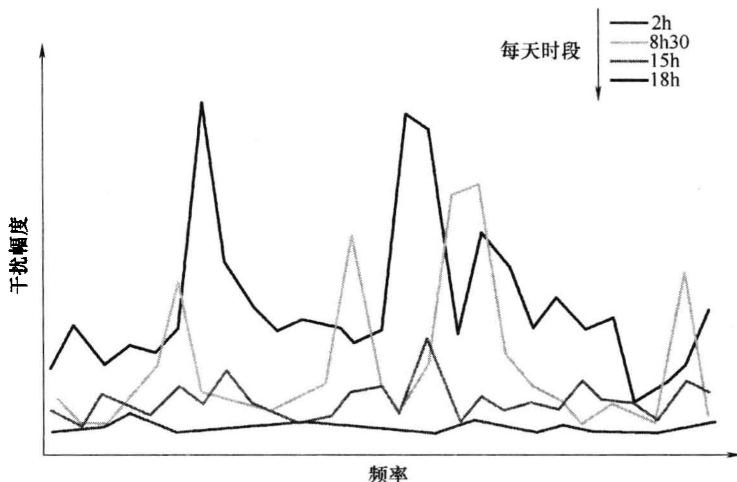


图 8.15 随日工作时间而变化的作用在室内电气网络上的干扰幅值

目前，这类技术已经获得了极大的提高，可以确保电力线上数据通信的可靠性。但是，对于与PLC设备使用同一个插座上的某些电气设备（例如卤素灯、真空吸尘器等），还是有必要采取一定的预防措施。

图8.16给出了如何同时使用PLC设备和接线板。对于PLC设备来说，接线板本身就是一个噪声源，且连接在接线板上的干扰性设备所产生的噪声会在该设备上产生叠加效应。任何情况下，只要有可能，均应该首选将PLC设备直接连接在墙上的插座之上或者连接至某个“biplite”（双插座接线板）。

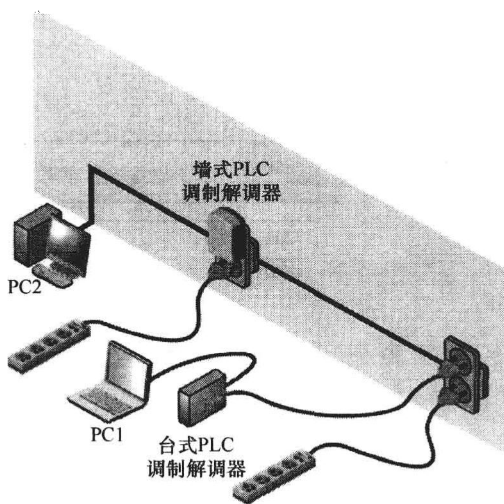


图8.16 接线板和双路插座的最佳使用方法

8.5 网络的数据传输速率

除了存在电磁干扰之外，PLC网络还存在与其技术本身有关的限制。这些与限制相关的数据传输速率与期望的数据传输速率和安全性并不一致。

HomePlug 1.0 网络的理论数据传输速率在1～14Mbit/s之间。14Mbit/s的数据传输速率仅为一个理论值，其相应的有用数据吞吐量约为5Mbit/s，即0.625MB/s。HomePlug Turbo 和 AV 的理论数据传输率分别为5～85Mbit/s和10～200 Mbit/s，相应地，有用数据吞吐率则分别为1～20Mbit/s和5～60Mbit/s。

HomePlug 所使用的帧头大小以及用于在电气环境中确保能够可靠传输数据的大量机制，大体上可以解释这一判别。传输数据中，有一部分是用于控制和管理传输工作，使得传输更加可靠。设备所提供的数据传输率中，仅有一部分是用于传输数据本身。

8.5.1 有用数据吞吐量的计算

有用数据吞吐量分别对应于OSI层（多个层）的数据传输速率。第1、2和3层等的有用数据吞吐量以及这些层相应的数据传输速率，可以根据管理和发送这些被传输数据所需要的开销来计算。

如第5章所述，通过该电气接口所发送的数据与物理帧也就是PLCP-PDU是相一致的。这种帧由PLCP帧头和来自MAC层的数据这两大部分组成，且帧头有两

个子部分组成。如图 8.17 所示，PLCP-PDU 各大部分的发送速率各不相同。

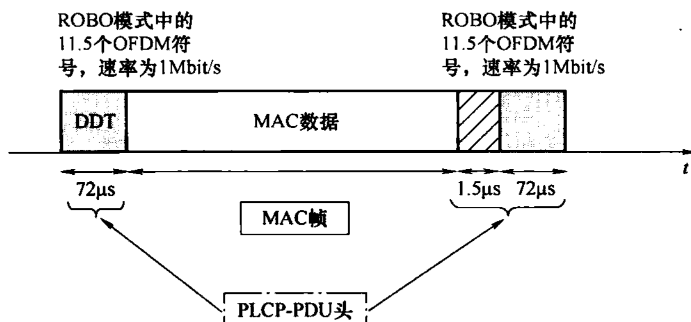


图 8.17 PLCP-PDU 的结构

PLCP-PDU 的帧头包含有起始和终止定界符。前导部分较长时，帧头的传输速率为 1Mbit/s。

PLCP-PDU 的第二大部分对应于 MAC 帧本身。对于 HomePlug 1.0 来说，其帧的发送速率可以高达 1～4.5Mbit/s、9Mbit/s 或者 14Mbit/s。PLC 本身拥有一个数据传输速率调整机制，可以根据电气环境的特性，以不同的传输速率进行数据传输。在计算第 2 层有用数据吞吐量时，必须事先知道传输时间。传输时间也就是用于发送数据信号的时长。由于使用电气接口作为传输介质，且电子在电力线上的运动速度相当于光速，因此信号在电力线上的传播时间可以视为 0。这样传输时间（Tt）相当于数据发送所需要的时间。

根据定义，第 2 层有用数据吞吐量 Du 相当于被传输数据负荷总量除以总传输时间，即

$$Du = \frac{Data}{Tt}$$

倘若认为 HomePlug 1.0 网络使用较短的前导（Preamble），且该网络中所有工作站的传输速率均为 14Mbit/s 时，我们就可以据此计算出可以发送 1500B 数据的 PLCP-PDU 的有用数据吞吐量（Du_1）。尽管数据负荷总量（为 1500B）大小已知，但是用于传输 PLCP-PDU 帧头和传输 MAC 数据的时长总和仍旧需要计算。

MAC 帧包含有一个 34B 的帧头[⊖]。因此，MAC 帧的大小为 1534。故它们的传输时间（Tt_{MAC}）可以根据下式计算：

$$Tt_{MAC} = \frac{1534\text{B} \times 8\text{bit/B}}{14\text{Mbit/s}} \approx 0.000876\text{s}$$

PLCP-PDU 帧头的大小总计为 120bit，发送速率为 1Mbit/s，故 PLCP-PDU 帧

⊖ MAC 帧包括 MAC header 和数据两部分。——译者注

头的传输时间为

$$Tt_{PLCP-PDU} = 72\mu s + 1.5\mu s + 72\mu s = 145.5\mu s$$

因此，总传输时间（Tt_1）为

$$Tt_1 = Tt_{MAC} + Tt_{PLCP-PDU} \approx 0.0010215s$$

在传输的数据中，有用数据吞吐率等于需传输的信息总量即 1500B（也就是 12000bit）除以上述传输时间（即 大约 1.021ms），相当于 11.74Mbit/s：

$$Du_1 = \frac{1500B \times 8bit/B}{Tt_1} \approx 11.74Mbit/s$$

然而，这个数据传输率与实际情况并不一致。在 PLC 中，数据的发送必须符合与 CSMA/CA（带有冲突避免的载波侦听多路访问）访问方式有关的某些规则。有关的访问方式的基础是第 3 章详述的某些机制，并可能产生相对较大的开销。

在单个工作站通过介质发送数据这一理想情况下，当工作站需要发送数据时，它首先会侦听介质。如果介质空闲可用，该工作站会延时一个 CIFS 时间然后进行传输。过了 CIFS 时间之后，如果介质仍然空闲可用，则该工作站会开始传输它的数据。数据传输结束之后，该工作站会再次等待一个 RIFS 时间，以等待该数据的确认信息。如图 8.18 所示，在这种传输方法中，应当重视确认信息和帧头传输所对应的 CIFS 和 RIFS 计时器所产生的开销，哪怕这个开销很小。

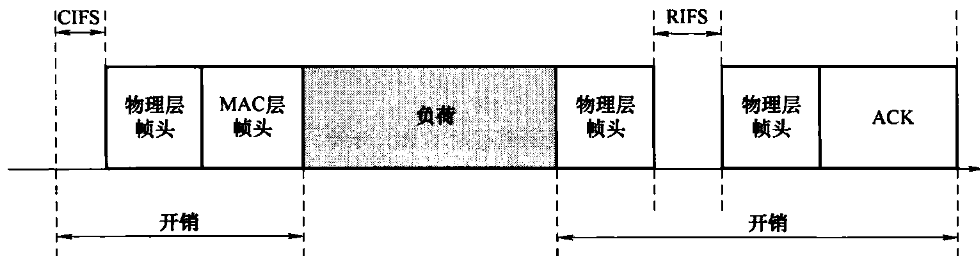


图 8.18 发送数据时的最小开销

现在，我们来计算这种理想情况下的有用数据吞吐量（Du_2）。如上例，考虑合适较短的前导信息，并以 14Mbit/s 的速率传输 1500B 的数据信息。

根据前面的计算，该数据传输时间相当于 Tt_1，即

$$Tt_{Data} = \frac{1534B \times 8bit/B}{14Mbit/s} + 145.5\mu s \approx 0.001670s$$

确认帧（ACK）的持续时间为 72μs，其传输时间等于

$$Tt_{ACK} = 72\mu s + 145.5\mu s = 0.0002175s$$

CIFS 和 RIFS 时长为定值。不过它们的值可以随着技术的不同而改变。在 HomePlug 1.0 中，CIFS 数值为 35.84μs；RIFS 数值为 26μs。

因此，总传输时间为

$$Tt_2 = \text{CIFS} + Tt_{\text{Data}} + \text{RIFS} + Tt_{\text{ACK}} = 0.001949\text{s}$$

所以，在这一理想情况下，有用数据吞吐量等于㊀

$$Du_2 = \frac{1500\text{B} \times 8}{Tt_2}\text{bit/B} = 6.157\text{Mbit/s}$$

我们可以发现，开销越大，有用数据吞吐量越小。由于该数据传输率对应于单工作站通过介质发送数据这一理想情况，因此，该数据传输率为有用数据吞吐量的最大值。

网络中含有多个工作站时，两个或两个以上的工作站有可能试图通过介质同时传输数据，这时，问题就变得非常复杂。某个工作站试图访问介质时，或者等待一个 CIFS 时间之后，如果它发现介质处于忙状态，且会推迟它的数据传输操作。为此，它会启动一个计时器，该计时器采用回退算法计算需要等待的时间。

额外的等待时间和随时回退计时器显然会使得开销更大，如图 8.19 所示。

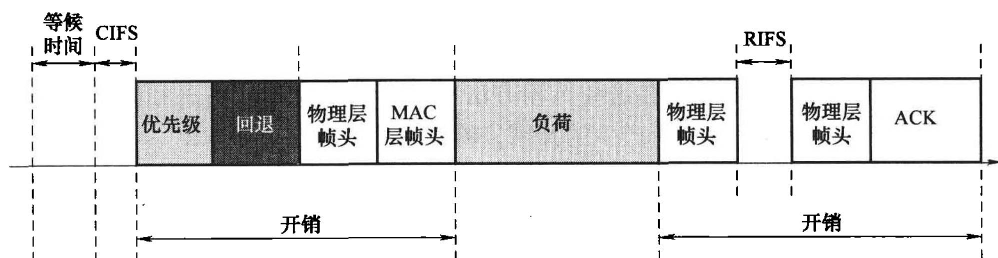


图 8.19 发送数据时的最大开销

这样一来，传输时间（Tt_3）变为㊁：

$$Tt_3 = T_{\text{Wait}} + \text{CIFS} + T_{\text{Backoff}} + Tt_{\text{Data}} + \text{RIFS} + Tt_{\text{ACK}}$$

由于等待时间和回退计时器的值不固定，所有很难确定具体的时间长度值。然而，在理想情况下，我们可以认为，等待时间与回退时间之和通常与传输时间相同。与等待时间相比，回退计时器的值很小，可以视为 0。等待时间数值上与另一个工作站的传输时间相同。

㊀ 原书在这一部分的计算存在错误。上页的 Tt_{data} 计算式显然是不正确的，并且 Tt_{ACK} 计算式的单位也是不正确的（单位应该为 s）。如果按照作者的计算方法，译者认为正确的计算过程应该为

$$Tt_{\text{Data}} = \frac{1534\text{B} \times 8\text{bit/B}}{14\text{Mbit/s}} \approx 0.000876\text{s},\quad Tt_{\text{ACK}} = 72\mu\text{s}$$

$$Tt_2 = \text{CIFS} + Tt_{\text{Data}} + \text{RIFS} + Tt_{\text{ACK}} = 1155.34\mu\text{s}$$

最终，$Du_2 = \frac{1500 \times 8}{Tt_2} = 10.387\text{Mbit/s}$。——译者注

㊁ 原书此处公式有编辑错误，现已更正。——译者注

因此，有用数据吞吐量等于[⊖]

$$Du_3 = \frac{Data}{Tt_3} = \frac{Data}{T_{\text{Wait}} + T_{\text{Backoff}} + Tt_2}$$

并可以进一步表示为

$$Du_3 \approx \frac{Data}{2Tt_2} = \frac{Du_2}{2}$$

网络由两个工作站组成时，每个工作站的有用吞吐量基本上等于最大有用吞吐量除以构成该网络的工作站的数量。该公式可以进一步推广并适用于由传输速率相同的 n 个工作站构成的 PLC 网络。因此，各个工作站的有用数据吞吐量等于

$$Du_3 \approx \frac{Du_2}{n}$$

需要注意的是，我们前面的计算中，仅考虑了第 2 层的有用数据吞吐量。然而，MAC 帧的数据中包含了一个 LLC 帧，这个帧的帧头为 4B，随后是一个 IP 封包（packet），并且此封包有 20B 的包头。IP 封包本身又是一个 24B 的 TCP 段（segment）。因此，额外的开销总计有 48B。更上层（例如第 3 层和第 4 层）在处理数据时，还会产生开销，这类开销我们在此不考虑。

结论很明显，PLC 网络始终无法达到物理介质声称的数据传输容量。根据我们实验，数据传输速度为 14Mbit/s 时，用户可用的数据总数量大约仅为电气接口原始速率的一半，即平均 5Mbit/s（625KB/s）。

表 8.9 简要地列出了各种类型局域网的有用数据吞吐量。

在介质传输速率相同的情况下，以太网的有用数据吞吐率要远远高于 PLC 网络的有用数据吞吐率。

表 8.9 局域网有用数据吞吐量

网　　络	理论上的数据传输速率/(Mbit/s)	有用数据吞吐量/(Mbit/s)
Ethernet 10	10	8.08
Ethernet 100	100	90.06
HomePlug 1.0	14	5.1
HomePlug Turbo	85	40
HomePlug AV	200	150

8.5.2 PLC 实际数据传输速率的最大值

在前述章节中，我们已经计算了 PLC 第 2 层的有用数据吞吐量。现在，我们开

⊖ 原书此处将 Tt_2 写作 Tt_1 是不准确的，这里已经改正。——译者注

始考虑较高的协议层。这里，我们使用了 Iperf 流量生成器。该工具可以从 http://dast.nlanr.net/Projects/Iperf/地址获得。

Iperf 可以生成任意类型的客户端—服务器流量。在我们的试验中，如图 8.20 所示，我们使用了以下设备：

1）IBM R50e 计算机，操作系统为 Windows XP SP2；

2）DELL Latitude D600 计算机，操作系统为 FreeBSD 5.4；

3）两台 PLC 调制解调器，与每一台计算机上的相应技术（HomePlug 1.0、Turbo、AV 和 Spidcom 200 等）相一致；

4）两条 5 类屏蔽式 FTP 以太网电缆；

5）标准的 4 插座接线板。

将客户端（192.168.1.100）、服务器（192.168.1.110）和接入点（192.168.1.120）配置在同一个网段内的地址。否则的话，它们之间无法进行通信。

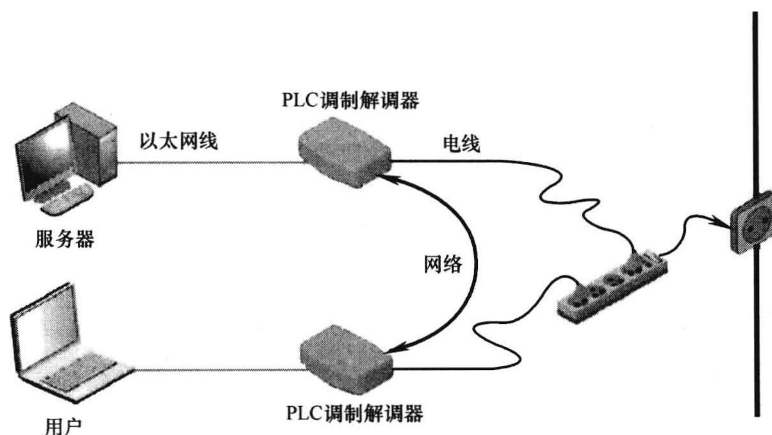


图 8.20 试验配置

该试验生成 100Mbit 的 TCP 流量，并根据数据传输网络和采用的机制，对相关的有用数据吞吐率进行验证。为了确保实验结果的可靠性，总共进行 3 次试验，并使用试验平均值进行验证，排除了过大的波动值。

在服务器端，所有工作仅需要启动一个 MS-DOS 控制台窗口，并在窗口内输入命令 iperf-s，完成服务器的初始化工作。在客户端，通过 MS-DOS 控制台窗口，输入命令 iperf-c 192.168.1.110-n 100000000，启动 100Mbit TCP 数据的传输工作。

表 8.10 为该试验台上各种技术所获得的实验结果。表 8.11 简要列出了某些常见因特网应用（数据、语音或者视频应用）所必需的数据传输速率。

表8.10 PLC技术的最大实际数据传输速率

标准或者技术	有用数据吞吐量/(Mbit/s)	最大实际数据传输速率/(Mbit/s)
HomePlug 1.0 (14Mbit/s)	5.1	4.35
HomePlug Turbo (85Mbit/s)	40	11.5
HomePlug AV (200Mbit/s)	150	60.5
DS2 (200Mbit/s)	150	61.2

表8.11 典型因特网应用所必需的数据传输速率

应 用	必要的传输速率
浏览因特网网页以及发送电子邮件 下行传输速率 上行传输速率	50kbit/s 5kbit/s
IP语音应用	80kbit/s
音频流应用 下行传输速率 上行传输速率	80kbit/s 14kbit/s
标清视频信道应用	1.5Mbit/s
高清视频信道应用	8Mbit/s

8.5.3 数据传输速率的变动

在PLC网络中，电气接口的相关限制可能会导致网络数据传输速率出现变动。如前所述，电力网络上的电气设备和众多的PLC设备都可能产生干扰，并因而导致数据传输速率出现波动。

环境中出现干扰时，PLC数据传输速率立即会自动地改变。该机制对用户是透明的。因此，HomePlug 1.0的数据传输速率从14.1Mbit/s可能变成12.83Mbit/s、10.16Mbit/s、8.36Mbit/s、6.35Mbit/s、4.04Mbit/s、2.67Mbit/s等。网络环境严重劣化的情况下，甚至于可能低至0.9Mbit/s。

对于支持数据传输速率自动变化方案的任意网络工作站，都可以为其赋予不同的数据传输速率。

图8.21给出了理论数据传输速率的变化过程以及使用Iperf工具通过试验所测得的有用数据吞吐量的变化过程。

对于由多个工作站组成的网络，我们已经知道，各个工作站的数据传输速率相当于最大有用数据吞吐量除以工作站的数量。然而，该结论的前提条件是，我们假

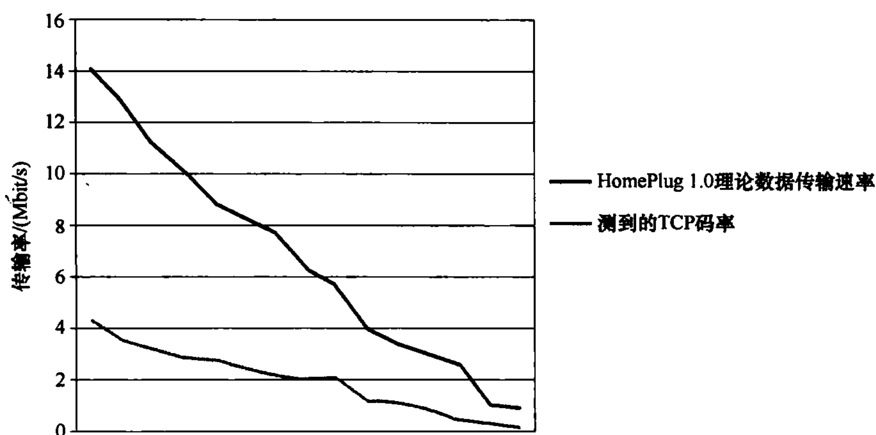


图 8.21 HomePlug 1.0 技术的理论数据传输速率和有用数据吞吐量的变动示意图

设所有工作站的传输速率均相等，且等待时间等于工作站的传输时间。

所有工作站的速率各不相同时，等待时间将会变长，并因而导致整个网络数据传输速率的急剧下降。网络上，如果某个工作站的传输速率为1Mbit/s，则其传输时间为传输速率为14Mbit/s的工作站的14倍。结果是，速度较快的工作站也必须等待为其等待时间的14倍时间之后，才能开始传输数据。由此可见，网络的平均有用数据吞吐量会趋向于1Mbit/s。

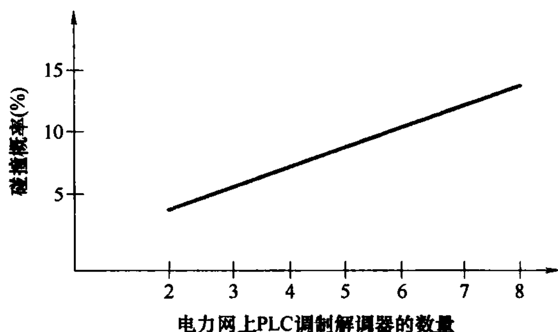


图 8.22 冲突概率与电力网络上 PLC 调制解调器数量之间的关系

图 8.22 给出了电力网络上的数据冲突概率与处于活跃状态的网络 PLC 设备数量之间的关系。

8.5.4 安全性

与 Wi-Fi 网络不同，由于 PLC 网络的介质无法接近（电力线敷埋在墙体之内，或者进行捆绑处理）且没有危险，因此，PLC 网络可以提供最高的安全等级。

一旦用户为其 PLC 网络设置了合适的密码，就可以实现这种程度的安全性能。在本书后续章节中，我们将详尽地描述如何配置 PLC 局域网。

第9章 配　置

PLC 网络的安装非常简单。所有工作仅需要在遵守前述章节所列出的限制条件下，将 PLC 设备连接至以太网或者某个调制解调器（ADSL、电缆、STN 等）即可。

网络安装完成之后，接下来需要对网络上的 PLC 设备及其所连接的终端接口（通常为 PC 的网卡）进行配置。本章将详细描述如何配置 PLC 设备以及所连接的终端的网卡。此外，还根据具体的应用场合（家用、专业、工业），对这些设备的各种功能进行了详细描述。

无论网卡是外置卡、以太网卡，还是 USB 卡，终端（PC）的配置均与网卡的安装及其软件配置有关。网卡的安装随操作系统的不同而不同。网卡的配置均是基于 PLC 技术（例如 HomePlug、DS2 等）所使用的参数，因此，在不同系统上的配置工作基本上相同。

尽管从 PLC 设备的市场占有率来看，HomePlug 规范是目前的 PLC 事实标准，后续章节还是按照当前的几种主要的 PLC 技术来描述需要配置的参数。

即使已经完成了网卡的配置，终端仍不能立即与网络进行通信。为了建立通信链路，还必须为网卡分配合适的网络参数，例如 IP 地址、子网掩码等。

9.1 HomePlug1.0 或 Turbo 网络的配置

当 PLC 网络使用 1.0 版 HomePlugTurbo 设备时，在某种程度上说，配置工作相对较为简单，这是因为，所有的网络设备在点对点模式的网络中都具有相同的层次性功能。HomePlug AV 设备所在的网络中，其中有一个设备是中央协调器（CCo），其他的则为站（STA）。然而，对于可以以同样的方式配置电力网络上所有的 HomePlugAV 设备的用户来说，这一点是透明的。

市面上符合 HomePlug 规范的所有设备均可以采用相同的方式进行配置，且它们之间彼此互相兼容。配置时，视目标操作系统的不同，可以选用各种不同的工具。

下面以 WindowsXP、Linux 和 FreeBSD 等操作系统为例进行说明。

在 Windows 下配置 PLC 网络

基本上所有的 HomePlug PLC 设备配置工具均拥有类似于 HomePlug 芯片参数配置功能的功能。从第 7 章可知，HomePlug 芯片主要源于制造商 Intellon 公司。它们

用于读取已经存储的、与 PLC 设备之间数据交换特性有关的各种大量数据。使用这些数据可以配置、优化 PLC 网络。

在各种可以配置的 HomePlug 参数之中，我们着重关注以下参数：

1）网络加密密钥（NEK），用于保证同一个 PLC 局域网内数据交换的安全性。

2）默认加密密钥（DEK），用于配置所有分布在电力网络上的远程 PLC 设备的网络加密密钥。

3）PLC 设备传输优先级，可以为 CA0、CA1、CA2 和 CA3 等 4 个值之中的某一个，用于配置某些 PLC 设备，例如连接至其他网络（尤其是以太网）的网关等。

表 9.1 简要列出了使用 HomePlug 工具，可以读取或显示给 PLC 网络用户主要参数。

表 9.1 配置工具可以查看的 HomePlug 参数一览表

HomePlug 参数	说　明
每 40 个符号的字节数	每个拥有 40 个 OFDM 符号的块的字节数量（用于为 HomePlug 1.0 计算被评估的物理层数据传输速率）
每个 336μs 块的字节数（适于 HomePlugTurbo）	每个 336μs 块的字节的数量（用于为 HomePlug1.1Turbo 计算被评估的物理层数据传输速率，有时候也称之为 Viper）
DATA_TX_COUNT	已传输数据数量计数器
接收到的错误帧	已接收到的错误类型帧的数量
帧丢弃	丢失帧的数量
ACK 计数器	已发送 ACK 类型帧的数量
NACK 计数器	已发送 NACK 类型帧的数量
FAIL 计数器	已发送 FAIL 类型帧的数量
冲突丢失计数器	已经丢失的冲突帧的数量
CA0 延时计数器	接收到 CA0 帧发送请求至成功访问传输信道所经历的总毫秒数
CA1 延时计数器	接收到 CA1 帧发送请求至成功访问传输信道所经历的总毫秒数
CA2 延时计数器	接收到 CA2 帧发送请求至成功访问传输信道所经历的总毫秒数
CA3 延时计数器	接收到 CA3 帧发送请求至成功访问传输信道所经历的总毫秒数
每 40 个符号字节数数据包累计计数器	以 40 个 OFDC 符号为计数单位的累计已接收帧的数量
MAC 地址	同一网络上其他 PLC 设备的 MAC 地址

PLC 设备间通信物理层数据传输速率评估

各种 PLC 设备均可以将设备交换过来的参数“每 40 个符号中的字节数”的瞬

时值存储在 HomePlug 芯片之内。如第 3 章所述，该数值用于评估 PLC 设备之间的物理层数据传输速率（在物理层）。

最大物理层数据传输速率必须与该数据量（位数）一致，从而确保使用持续时间为 8.4μs 的 40 符号的 OFDM 块来更好地进行调制。

由此可知，对于 HomePlug1.0 和 Turbo 来说，分别有

HomePlug 1.0：$Datarate_{PHYMAX}=\frac{519\times8}{40\times8.4}\text{Mbit/s}=12.35724286\text{Mbit/s}$

HomePlug Turbo：$Datarate_{PHYMAX}=\frac{2812\times8}{40\times8.4}\text{Mbit/s}=66.95238095\text{Mbit/s}$

我们仍然使用第 3 章中的数据，根据 HomePlug 芯片的相关参数，物理层数据传输速率的计算过程如下：

HomePlug 1.0

$$Datarate_{PHY}=\frac{588-38}{481}\times\frac{BYTES_{in40symbol}}{42}+\left(14-\frac{588-38}{481}\times\frac{519}{42}\right)\text{Mbit/s}$$

HomePlug Turbo

$$Datarate_{PHY}=\frac{BYTES_{per\ 336\mu s\ block}\times8}{40\times8.4}\text{Mbit/s}$$

式中，$BYTES_{per\ 336\mu s\ block}$表示在 336μs 的持续时间之内物理层数据块的字节数量。

从第 8 章可知，物理层数据传输速率与用户可用数据吞吐量之间存在着差别。由于 HomePlug PLC 配置工具仅为用户显示物理层数据传输速率，因此，在表 9.2 中，我们给出了这两个数据传输速率之间的估计对应关系。

表 9.2 被显示的物理层数据传输速率与可用数据吞吐量之间的对应关系

	物理层数据传输速率/(Mbit/s)	可用数据吞吐量/(Mbit/s)
HomePlug 1.0	14	4.5-5
	12.83	3.5
	11	3.2
	10.16	2.9
	8.36	2.4
	6.35	2
	4.04	1.22
	3	0.89
	1	0.33
	0.9（ROBO 模式）	0.2

（续）

	物理层数据传输速率/(Mbit/s)	可用数据吞吐量/(Mbit/s)
HomePlug Turbo	85	12.5
	75	11.8
	55	9.42
	45	8.79
	35	8.23
	25	7
	14	4.5
	12.83	3.5

HomePlug 1.0 和 Turbo PLC 有多种配置工具，在这些工具中，我们着重从用户界面和使用友好性等两个方面讨论以下工具：

1）MicroLink dLAN 和 MicroLink Informer，是 Devolo 公司的产品。前者用于配置 PLC 网络，后者用于检查网络状态。

2）PowerPacket 工具程序，是 Intellon 公司产品。该工具拥有各种标签，可以完成各种配置操作，能够实现与 Devolo 的工具相同的参数化操作（关于 PLC 逻辑网络的网络加密密钥，如图 9.1 所示；关于主要的 PLC 网络管理标签，如图 9.2 所示；关于各 VLAN 的优先级管理，如图 9.3 所示）。

3）SoftPlug，是 LEA-Thesys 公司的产品（http://209.236.239.167/Images/Upload/support_telechargement/SetupSoftPlug.msi）。

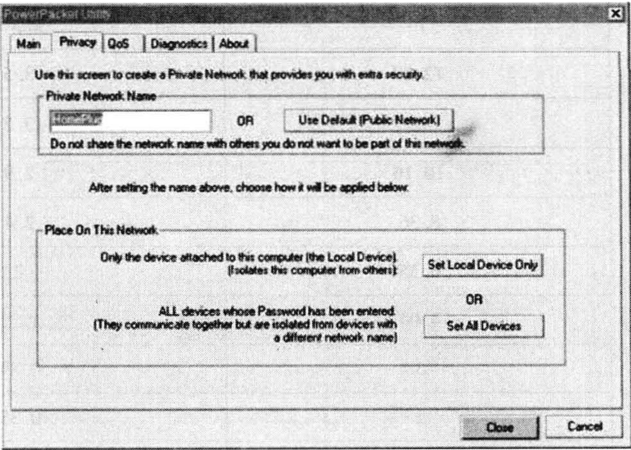


图 9.1 HomePlug 设备的加密密钥配置界面

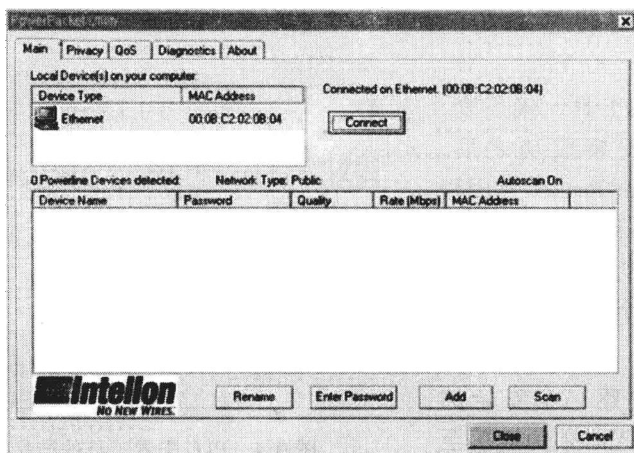


图 9.2 Intellon 公司的 PowerPacket 配置工具主要的标签页

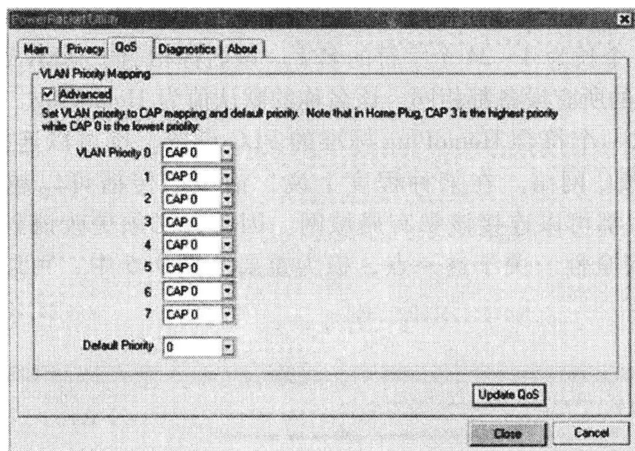


图 9.3 配置 HomePlug 中各个 VLAN 的优先级

与以前的工具相比，该工具可以提供相同的功能，但是，其界面更加容易使用。

大多数 PLC 调制解调器都有以太网接口。然而，某些 PLC 调制解调器提供 USB 接口，并使用该接口模拟“虚拟的”以太网接口。对连接终端来说，这些“虚拟的”以太网接口可以视作新的网络接口。

经证实，通过 USB 接口实现的虚拟网络接口工作不稳定，因此，建议为 PLC 设备配置以太网接口和 RJ-45 连接器。

以太网设备或者 USBPLC 设备的配置

我们选用 Intellon 公司的 Power Packet 实用程序配置工具为例，描述如何

完成与配置 PLC 设备相关的操作。

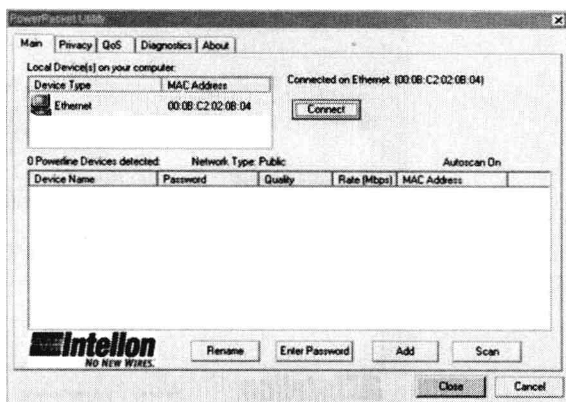


图 9.4　PLC 配置工具的产品标签页

首先下载该工具，接下来，安装该工具。安装成功之后，就可以启动 Power Packet 实用程序（通过开始→程序）。该工具程序有多个标签页，分别对应于不同的可用功能，如图 9.4 所示。

如果需要创建一个安全的 PLC 局域网，首先必须为连接至该网络上的所有设备配置网络加密密钥（NEK）。

在“Security（安全）”标签页，找到字段“Private network name（私有网络名称）”，并输入一个长为 4～24 个字符的名字。该名称相当于 NEK 密码。关于该名称，PLC 网络上的所有设备都相同。该名称的默认值为 HomePlug。

市售的任意一个符合 HomePlug 标准的 PLC 设备，都可以连接至 NEK 密码为该默认值的 PLC 网络。在某种程度上说，信号的传播可以越过房屋的电能表，因为任何人都可以连接该私有局域网。因此，必须更改该默认值，才能保证 PLC 网络的安全性。关于这一点，极为重要。图 9.5 中，可以看到该默认的密码。

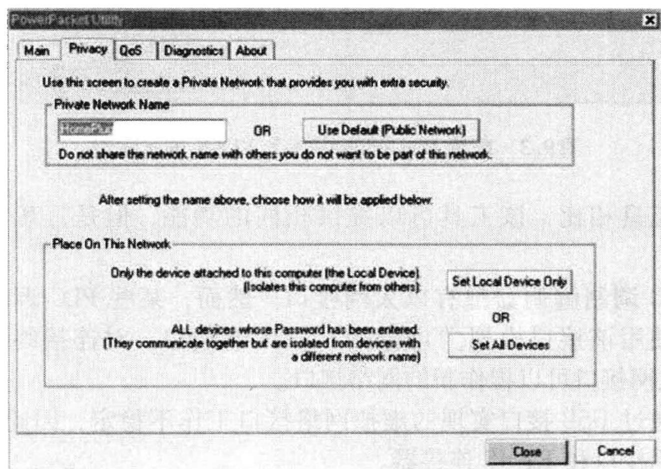


图 9.5　PLC 配置工具的安全标签页

在图9.6中，已经用新的PLC网络名称替换了默认的NEK密码。该密码越长，即密码中包含的数字和字符越多，试图非法访问该PLC网络的入侵者破解该密码的难度也就越大。

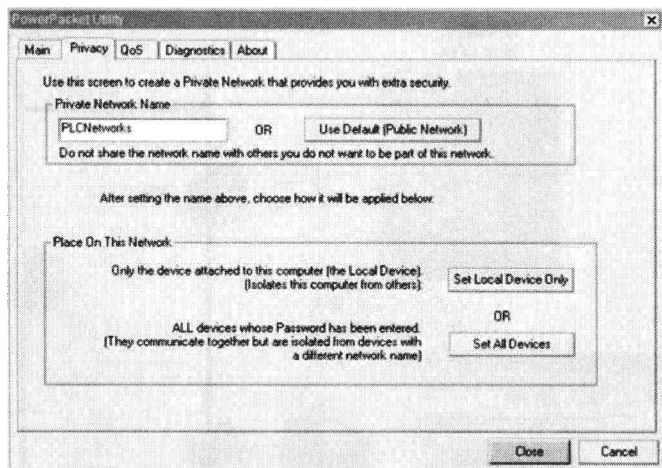


图9.6 配置PLC局域网的密码

对于连接至电气网络的所有PLC设备，无论是否已经存在于该PLC局域网之内，使用该配置界面都可以完成其配置操作。对于连接至电气网络上的远程设备，您需要做的仅是获得该设备的网络加密密钥。

每一个PLC设备的默认加密密钥（DEK）都是唯一的，且其ID标识在设备的底部。它通常被命名为SecureID（Devolo公司）、Password（Corinex和Oxance公司）、Mot de passe（Lea公司），也可能被命名为其他名字。密钥进行了编码处理，长为16个字节，采用十六进制格式。

需要配置的PLC设备的MAC地址的上面，可以找到默认加密密钥，图9.7所示设备的默认加密密钥的值为JJMZ-QFDI-RVHE-OJRS。该默认加密密钥进行了加密处理。

如果已经知道了默认加密密钥（DEK）值，则仅需要单击标签页“Add Products（添加产品）”，并将该值输入至字段“Password（密码）”之内。设备名称一栏



图9.7 从PLC设备的外壳上读出默认加密密钥（DEK）

则可以用来标识 PLC 设备（例如起居室或者寝室等）。

图 9.8 图示了 PLC 局域网的配置过程。其中，配置时使用的 DEK 相应地从连接至同一个电力网络上起居室设备和寝室设备的外壳上读出。

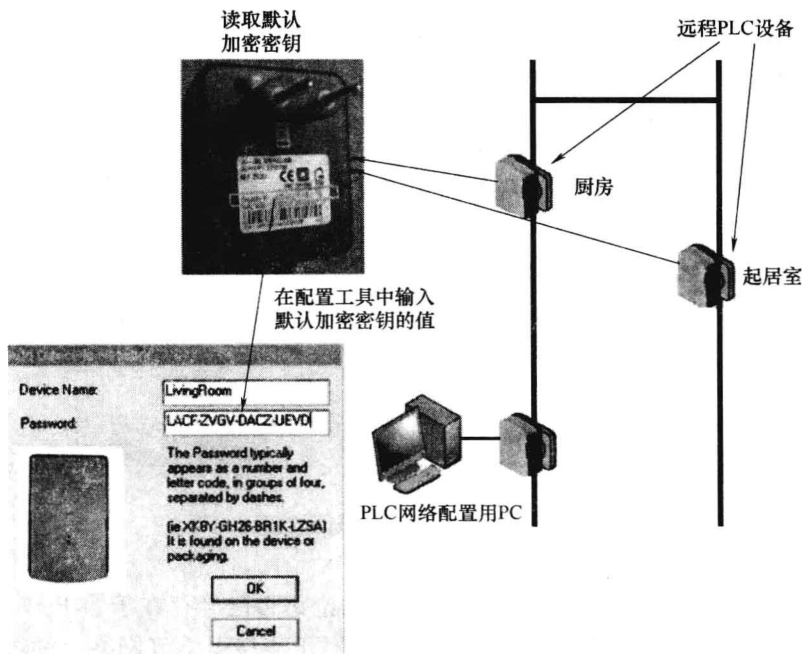


图 9.8　使用默认加密密钥配置 PLC 网络

以本地方式或者使用 DEK 密钥完成所有联网 PLC 设备的配置之后，仅需简单地选择“Products（产品）”标签页，就可以检查 PC 所连接的设备与已经连接至该电力网络上的其他 PLC 设备之间的 PLC 链路的状态（见图 9.9）。

1）窗口“Product（s）connected to your PC（您的 PC 已经连接的产品）”显示通过 PC 的网卡及其 MAC 地址，直接以太网连接至该配置用 PC 的 PLC 设备。

2）窗口“Product（s）sensed（已经检测到的产品）”则列出电力网络上已经检测到的、拥有相同网络加密密钥的所有 PLC 设备。此外，该窗口还显示这些 PLC 设备的数据传输率估计值。

单击“rename（重新命名）”，可以为该列表中的产品重新命名；给出一个相关名称，还可以检索该电力网络架构中的 PLC 设备。图 9.9 中的 PLC 设备已经被重新命名为起居室和寝室。

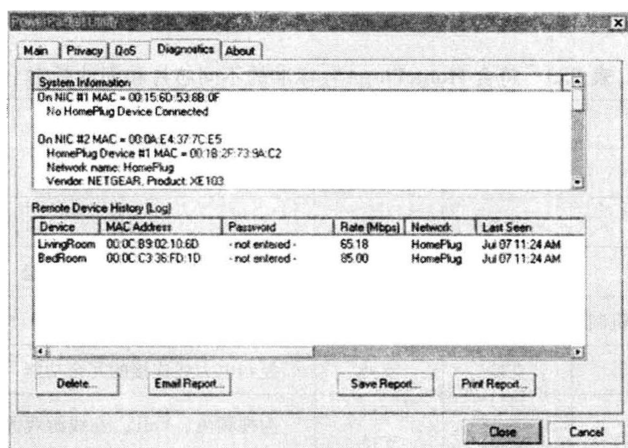


图9.9 PLC 网络状态诊断功能

同一个电力网络上多个 HomePlug PLC 局域网的共存

同一个 HomePlug1.0 和 TurboPLC 设备上，不得配置多个网络加密密钥。因此，同一个设备不得同时属于多个 PLC 局域网。在 HomePlugAV 规范的框架之内，同一个 PLC 设备可以具备多个加密密钥，因此，同一个 PLC 设备可以同时属于多个 PLC 局域网。

同一个电气网络上，可以拥有多个 PLC 局域网。这些 PLC 局域网会共享频段(从 1 ~ 30MHz)，并按照已有 PLC 局域网的数量平分传输速率。

完成 PLC 网络的配置工作之后，就可以为包含该 PLC 网络的以太网的用户配置 IP 网络和合适的应用了。关于 IP 网络的配置，详细情况见第 10 章。

单击标签页“Diagnostics（诊断)”，可以显示 PC、通过以太网直接连接至该 PC 上的 PLC 设备等相关信息。此外，还显示了该配置工具早期已经检测到的 PLC 产品的历史信息。

图 9.9 给出了该标签页。在该标签页中，显示了与该 PLC 网络（PLCNetworks）有关的寝室设备，以及上一次显示该设备的日期和时间。单击“Print（打印)”，可以将这些历史信息保存并发送至其他的 PLC 网络安装程序。

9.2 配置 HomePlugAV 网络

HomePlugAV 标准基于 Intellon 公司生产的两种芯片（分别集成了版本为 1.0 和 1.1 的固件）所确立的规范，可以使用多个标准实现方案。

表 9.3 对比了基于 Intellon 公司的芯片 INT6000 和 INT6300 实现的两个版本之

间的功能差别。

表 9.3　符合 HomePlugAV 标准的不同芯片和固件版本

功　能	1.0	1.1	优　点
芯片	INT6000	INT6300	
固件	1.x	3.x	
128bit 加密	支持	支持	为电力线网络提供安全功能
CSMA/CA 信道访问机制	支持	支持	提供可靠的网络连接
CCo 故障切换	支持	支持	控制电力线连接的冗余功能
QoS（VLAN、TOS）	支持	支持	为视频流、VoIP、在线游戏等服务提供更好的用户体验
轮换式 NEK 加密算法	支持	支持	提供高度安全的电力线网络
IGMP v3	不支持	支持	提供高效的网络连接
信号强度 LED 指示灯	无	有	是一个极佳的电力线网络现场检查工具
单键加密	不支持	支持	使用极为友好，用于启动加密
复位至工厂默认设置	不支持	支持	使用极为友好，用于部署住宅网络时执行复位功能

为了使终端用户可以更加方便地配置 PLC 网络，促进因特网服务提供商使用 PLC 技术通过网络电视向家庭环境提供高清电视广播服务。可以使用两种 PLC 网络配置模式：

1）通过 PC 上的嵌入式用户界面或者因特网接入网关（通常通过网关的 Web 界面）进行配置。

2）通过用于快捷部署 HomePlug AV PLC 网络的 EasyConnect 模式进行配置。该模式需要使用配有 INT6300 芯片的 HomePlug AV PLC 设备所安装的连接按钮。配置新网络时，首先必须按下第一个设备上的该按钮，并持续 2s。

外壳上的电源指示灯会点亮，稍后会闪烁。此后，对于想添加至用户的逻辑 PLC 网络的其他设备，用户必须在 1min 之内按下这些设备上的 EasyConnect 按钮。其他设备上的该按钮也必须持续按压 2s，以将它们关联至第一个设备。设备关联完成之后，各个网络站上的 PLC 工作指示灯将处于持续点亮状态；此后，可以开始 PLC 网络的配置工作。图 9.10 描述了使用 EasyConnect 模式，将新站关联至 PLC 网络的工作原理。

关于 HomePlug AV PLC 网络的配置工具，可以根据具体的制造商，使用不同的用户界面，对各种设备的加密密钥和优先级采用不同的管理工具。其中的一些工具如下所述：

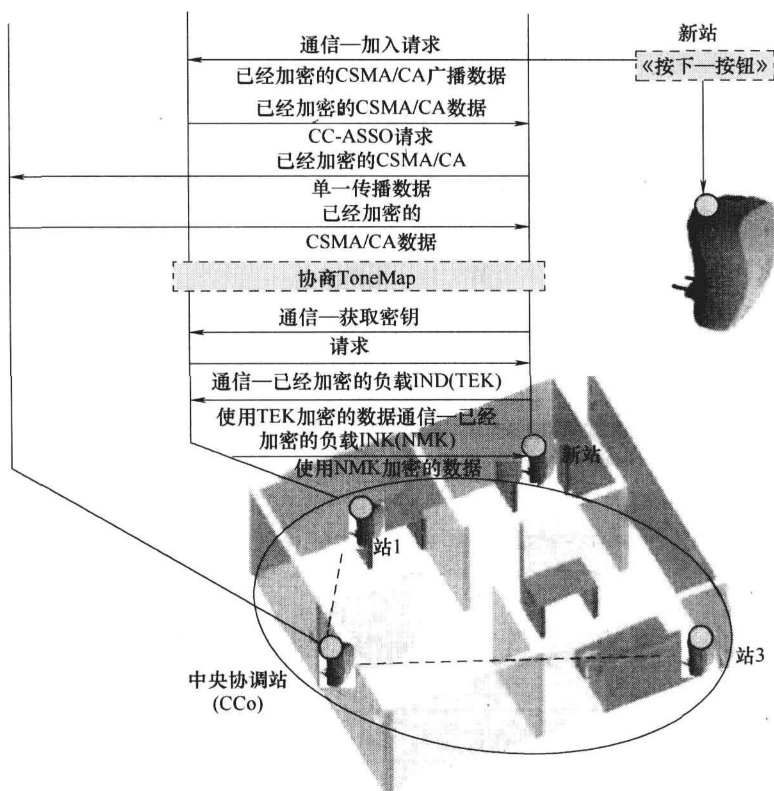


图9.10 使用 EasyConnect 模式实现 HomePlug AV PLC 设备关联的原理

1) AZtech HomePlug AV Utility（下载地址为 ftp://ftp. aztech. com/support/malayia/HomePlug/HL108E%20HomeplugAV%20Utility%20v1. 0. zip）;

2) Zyxel PLAPLAtool（下载地址为 http://us. zyxel. com/upload/download_library/PLA-470_3. 0. 5（AP). zip）;

3) Devolo dLAN Software（下载地址为 http://download. devolo. net/webcms/0155878001190908944/dlan-software-v17. exe）;

4) Linksys PLE 200 Utility（下载地址为 ftp://ftp. linksys. com/downloads/NA/firmare/PLE200%20FW3. 3%20Rev2%20NA. zip）;

5) AsokaUSAPowerManager（下载地址为 http://asokausa. com/downloads/PowerManager1. 2. 0-Common. zip）。

AsokaUSA 开发的工具部署容易，用户界面友好，因此，在配置实例中，我们将使用该工具。工具程序 Power Manager 启动之后，会弹出一个窗口，可以选择该工具程序要使用的网卡，如图 9. 11 所示。

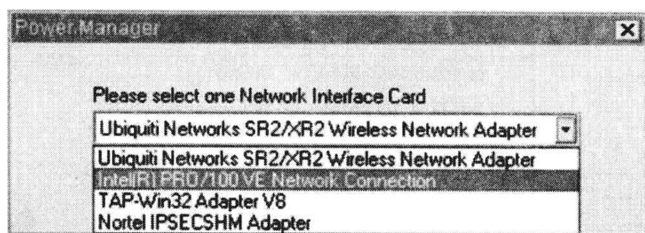


图 9.11 选择网卡

此后，安装程序开始安装驱动程序，以更好地处理发送至 PLC 设备的帧，如图 9.12 所示。

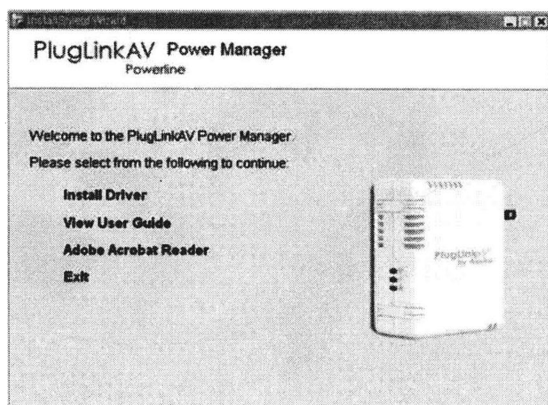


图 9.12 选择需要安装的 PLC 工具模块

PLC 工具安装程序 Power Manager 自启动至安装完成，需要完成多个安装步骤（见图 9.13）。

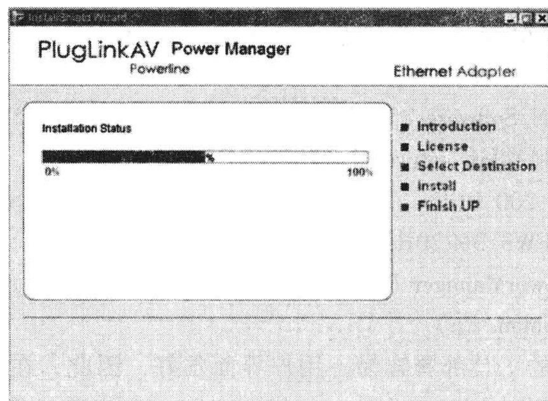


图 9.13 PLC 工具安装进度

安装过程完成之后，Power Manager 工具会立即弹出一个窗口，提示重新命名连接至安装用 PC 机上的 PLC 设备（见图 9.14），并为其指定一个设备名称。使用该设备名称，在 PLC 逻辑网络管理器中可以方便地查找该设备的标识符。

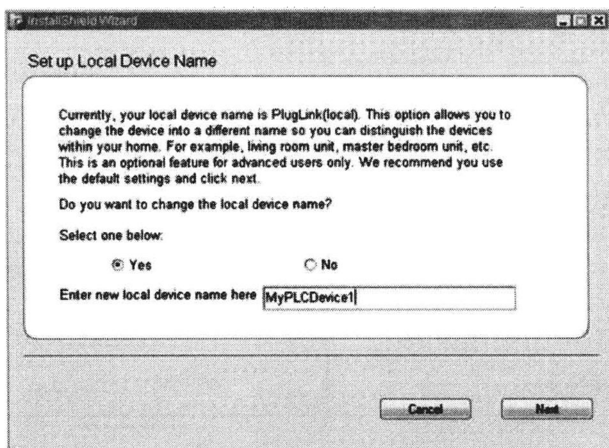


图 9.14 重新命名连接至配置用 PC 的本地 PLC 设备

接下来可以配置本逻辑 PLC 网络的全部 PLC 设备的网络加密密钥（NEK）。如图 9.15 所示，在这里，我们使用 HomePlug123 作为网络加密密钥（NEK）。

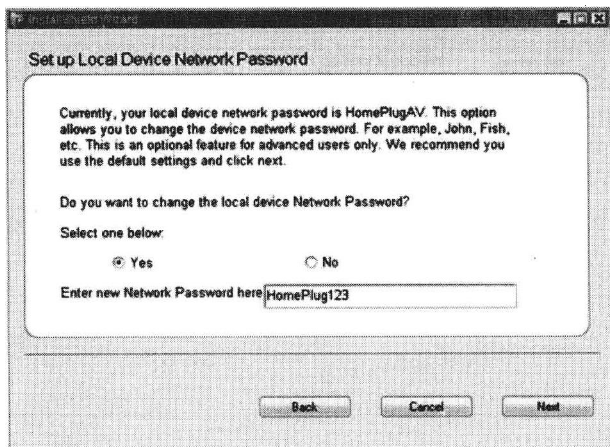


图 9.15 为 PLC 逻辑网络配置网络加密密钥（NEK）

此后，将进入该 PLC 工具的主界面。主界面中，有各种图标命令，可以完成设备配置文件的管理、逻辑网络上已有设备的管理、固件版本的更新、设备间 PLC

链路的分析统计等各种功能，如图 9. 16 所示。

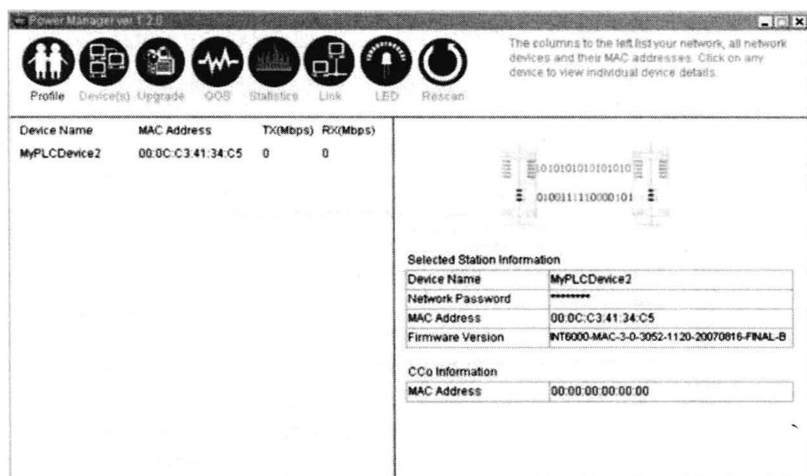


图 9. 16 Power Manager 工具的主标签页

使用标签页“Devices（设备）”，可以方便地查看已经配置的设备，还可以为它们分配新的参数（例如它们的名称或者网络加密密钥等），如图 9. 17 所示。

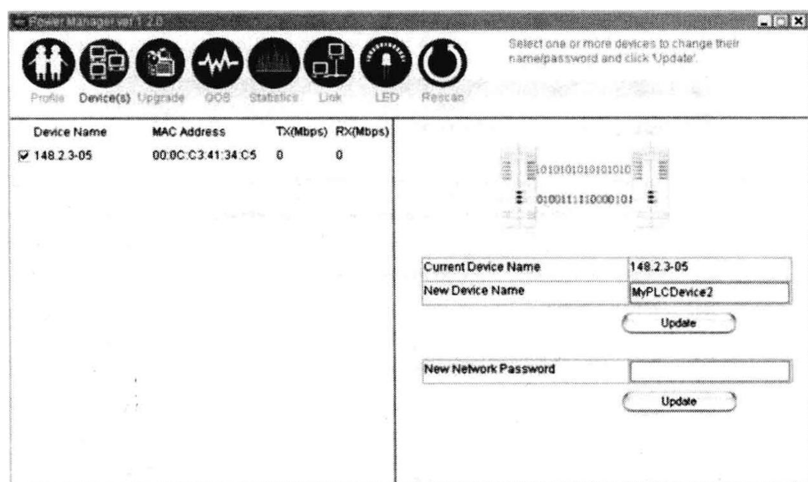


图 9. 17 Power Manager 工具的“设备”标签页

对于远程 PLC 设备，也可以查看电力网络上使用了默认加密密钥的远程设备的网络加密密钥，如图 9. 18 所示。

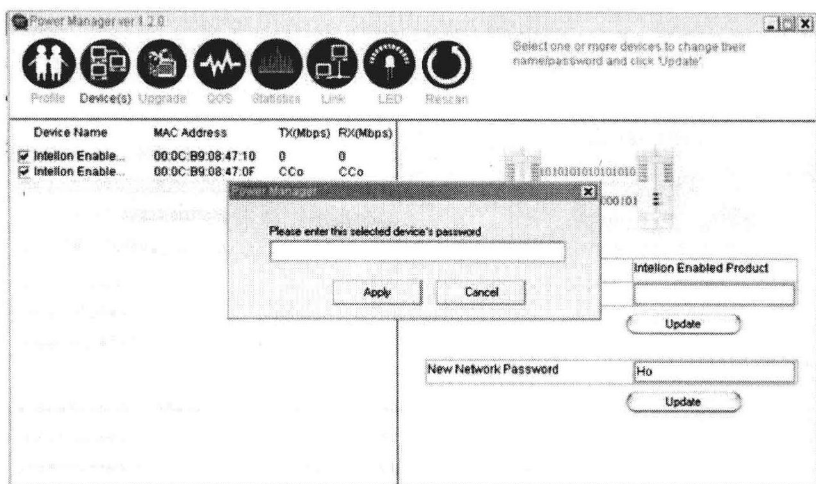


图 9.18　为远程设备配置 DEK 密钥

按照前面第 7 章和第 8 章所描述的安装要求，利用工具程序 Power Manager 的全部功能，可以方便地完成 HomePlugAV 网络的安装、配置和监控等操作。

9.3　在 Linux 下配置 HomePlug1.0PLC 网络

与在 Windows 操作系统中相同，在 Linux 中安装 PLC 网络也同样包括两个步骤，第一，将 PC 的网卡连接至电力网络上某个 PLC 设备之上，第二，使用 Linux 版的 PLC 配置工具完成配置工作。

如果 PLC 设备使用的是 USB 接口，则必须安装以太网 USB 虚拟接口的驱动程序。为此，必须通过以下地址下载、恢复含有该驱动程序的文件（适用于 Devolo 设备）：

http://download.devolo.biz/webcms/0607105001130251610/dLAN-linux-package-2.0.tar.gz（图 9.19 为 Devolo 网站的网页）。通过该页面，可以下载 dLAN duo 设备的 PLC 配置工具。

单击链接 “Driver Linux” 开始下载该工具程序，当出现如图 9.20 所示的下载窗口时，通过设置，将文件保存在磁盘中的某个位置。

实例中，我们将该文件保存在以下目录之内：

```
carcelle@ debian:~/Projects/CPL
```

文件下载成功之后，使用以下命名，对该文件执行两次解压操作：

```
carcelle@ debian:~/Projects/CPL $ gunzIPdLAN -linux -package - 2.0.tar.gz
carcelle@ debian:~/Projects/CPL $ gunzIPdLAN -linux -package - 2.0.tar.gz
```

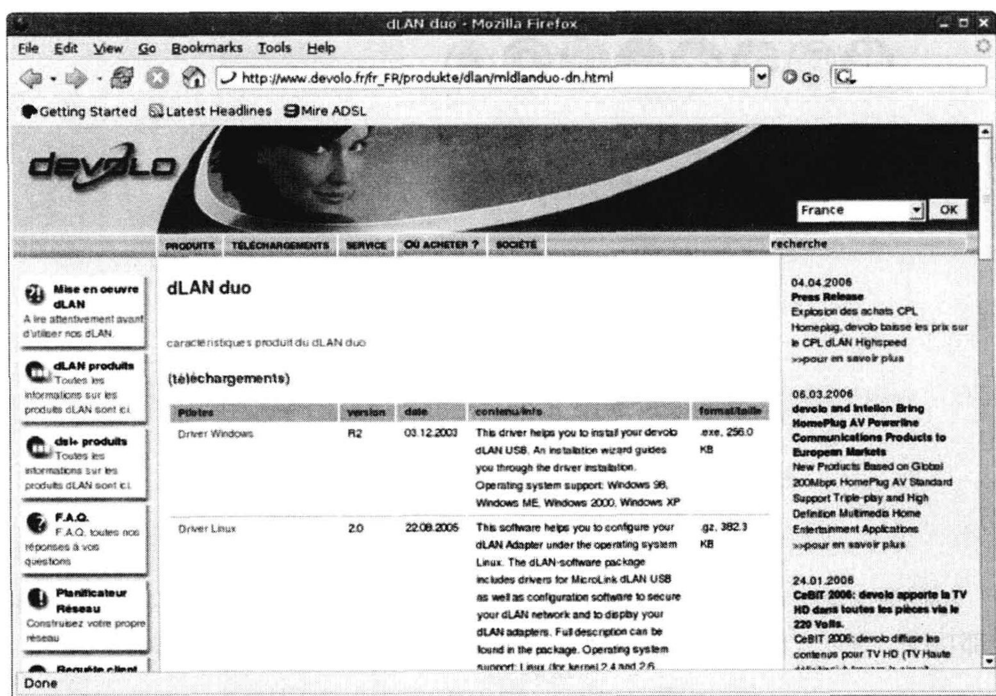


图 9.19　Devolo dLAN duo 设备的配置工具的主页

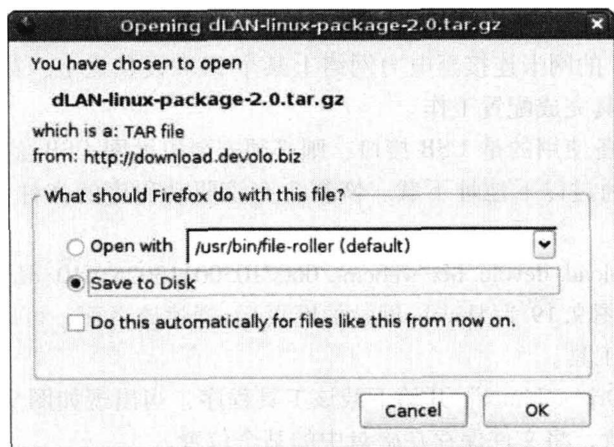


图 9.20　Linux 操作系统中 PLC 工具的下载窗口

此时，必须将 USBPLC 设备连接至 PC 上的可用端口。接下来，运行以下命令，对设备的识别情况进行验证：

```
carcelle@ debian:~ /Projects /CPL $ dmesg
```

命令“dmesg”的运行结果如图9.21所示。

```
carcelle@debian: ~
Fichier Édition Affichage Terminal Onglets Aide
pcmcia: see http://www.kernel.org/pub/linux/utils/kernel/pcmcia/pcmcia.html for
details.
hw_random: RNG not detected
ACPI: Battery Slot [BAT0] (battery present)
ACPI: AC Adapter [AC] (on-line)
ACPI: Power Button (FF) [PWRF]
ACPI: Lid Switch [LID]
ACPI: Sleep Button (CM) [SLPB]
NET: Registered protocol family 10
lo: Disabled Privacy Extensions
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 5
devolo_usb: module license 'devolo AG' taints kernel.
Driver for MicroLink dLAN USB:v2.0
usbcore: registered new driver devolo
[drm] Initialized drm 1.0.0 20040925
ACPI: PCI Interrupt 0000:00:02.0[A] -> Link [LNKA] -> GSI 11 (level, low) -> IRQ
 11
[drm] Initialized i915 1.1.0 20040405 on minor 0:
[drm] Initialized i915 1.1.0 20040405 on minor 1:
mtrr: base(0xe0020000) is not aligned on a size(0x300000) boundary
usb 2-1: new full speed USB device using uhci_hcd and address 3
usbcore: registered new driver cdc_ether
carcelle@debian:~$
```

图9.21 dmesg命令的运行结果

进入PLC工具的解压目录，按照以下方法安装已经下载的驱动程序：

carcelle@ debian:~/Projects/CPL $ cd dLAN - linux - package - 2.0/driver/

该目录所包含的文件如图9.22所示。

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/driver
Fichier Édition Affichage Terminal Onglets Aide
carcelle@debian:~$ cd Projets/
carcelle@debian:~/Projets$ kls
bash: kls: command not found
carcelle@debian:~/Projets$ ls
CPL                  dLAN_Install_6.png       Synaptics_Install_4.png
dLAN_Install_10.png  dLAN_Install_7.png       Synaptics_Install_5.png
dLAN_Install_11.png  dLAN_Install_8.png       Synaptics_Install_6.png
dLAN_Install_12.png  dLAN_Install_9.png       Syn_Install_DLAN1.png
dLAN_Install_13.png  Synaptics_Install_1.png  Syn_Install_DLAN3.png
dLAN_Install_4.png   Synaptics_Install_2.png
dLAN_Install_5.png   Synaptics_Install_3.png
carcelle@debian:~/Projets$ cd CPL
carcelle@debian:~/Projets/CPL$ ls
dlanethernet.jpg  dLAN-linux-package-2.0  dLAN-linux-package-3.0.tar
carcelle@debian:~/Projets/CPL$ cd dLAN-linux-package-2.0/
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0$ ls
config.log     driver                                          Makefile.in   tool
config.status  install.sh                                      Makefile.old
configure                  libpcap-0.8.3.tar.gz  Makefile      README
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0$ cd driver/
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ ls
devolo          devolo_usb.h   devolo_usb.mod.c  devolo_usb.o    Makefile
devolo_usb.c    devolo_usb.ko  devolo_usb.mod.o  installboot.sh  Makefile.in
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$
```

图9.22 USBPLC设备驱动程序目录内的文件

此时，必须切换为超级用户（根用户）模式，并运行安装命令 install. boot. sh（见图 9. 23）。

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/driver
Fichier  Edition  Affichage  Terminal  Onglets  Aide
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0$ cd driver/
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ ls
                              devolo_usb.mod.c  devolo_usb.o    Makefile
                devolo_usb.ko  devolo_usb.mod.o
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ sudo make
make -C /lib/modules/2.6.15-1-686/build SUBDIRS= modules
make[1]: Entering directory `/usr/src/linux-headers-2.6.15-1-686'
  CHK     include/linux/version.h
  HOSTCC  scripts/basic/fixdep
gcc: scripts/basic/fixdep.c: No such file or directory
gcc: no input files
make[2]: *** [scripts/basic/fixdep] Error 1
make[1]: *** [scripts_basic] Error 2
make[1]: Leaving directory `/usr/src/linux-headers-2.6.15-1-686'
make: *** [default] Error 2
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ sh installboot.sh
Starting boot-installing procedure...

You must be root to (un)install the boot script
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ sh installboot.sh
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$
carcelle@debian:~/Projets/CPL/dLAN-linux-package-2.0/driver$ su
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver# sh installboot.sh
```

图 9. 23　运行安装命令

下一步，必须运行命令 make usbdriver，完成 USB 驱动的编译（见图 9. 24）：

carcelle@ debian: ~ /Projects /CPL /dLAN-linux-package-2.0 /driver $make usb-driver

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier  Edition  Affichage  Terminal  Onglets  Aide
checking for select... yes
checking for socket... yes
checking for strerror... yes
checking for vfork... yes
checking for fork... yes
configure: creating ./config.status
config.status: creating Makefile
config.status: creating tool/Makefile
config.status: creating driver/Makefile
config.status: creating tool/config.h
config.status: tool/config.h is unchanged
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make usbdriver
making all in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-pack
age-2.0/driver »
make -C /lib/modules/2.6.15-1-686/build SUBDIRS=/home/carcelle/Projets/CPL/dLAN-
linux-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
  Building modules, stage 2.
  MODPOST
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-
2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# █
```

图 9. 24　运行命令 make usbdriver

编译成功地完成之后，运行以下命令（见图9.25），将驱动程序安装在合适的磁盘目录之内（见图9.26）：

```
carcelle@ debian: ~ /Projects /CPL /dLAN-linux-package-2.0 /driver $make
install-usbdrive
```

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier  Édition  Affichage  Terminal  Onglets  Aide
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-pack
age-2.0/driver »
make -C /lib/modules/2.6.15-1-686/build SUBDIRS=/home/carcelle/Projets/CPL/dLAN-
linux-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
  Building modules, stage 2.
  MODPOST
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-
2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install-usbdriver
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko /lib/modules
/2.6.15-1-686/extra
/sbin/depmod -a &&      /sbin/modprobe devolo_usb

In order to have your usb driver running and configured
at boot, you should go into driver directory and type

    make installboot

make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0#
```

图9.25　运行命令 make install-usbdriver

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier  Édition  Affichage  Terminal  Onglets  Aide
2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install-usbdriver
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko /lib/modules
/2.6.15-1-686/extra
/sbin/depmod -a &&      /sbin/modprobe devolo_usb

In order to have your usb driver running and configured
at boot, you should go into driver directory and type

    make installboot

make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# cd driver/
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver# make installboot
Starting boot-installing procedure...
Debian /etc/
installing devolo in /etc/init.d....
creating link to devolo in /etc/rc2.d
creating link to devolo in /etc/rc3.d
creating link to devolo in /etc/rc5.d
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver# cd ..
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# reboot
```

图9.26　运行命令 make install-boot

最后，运行下一个命令：

carcelle@ debian: ~/Projects/CPL/dLAN-linux-package-2.0/driver $make in-stallboot

使得计算机开机时，自动加载该 USB 驱动。

重新启动计算机，验证所有的命令是否运行成功。

重启结束时，该设备必须仍然连接在 USB 端口上。使用图 9.27 所示命令，检查并确认该新的 USB 以太网虚拟网卡已经安装成功。网卡 dlanusb0 确实已经安装好（见图 9.27）。此时，我们可以开始安装配置工具程序。

```
carcelle@debian: ~
Fichier  Édition  Affichage  Terminal  Onglets  Aide
carcelle@debian:~$ sudo ifconfig -a
dlanusb0  Link encap:Ethernet  HWaddr 00:08:38:0D:6A:89
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

eth0      Link encap:Ethernet  HWaddr 00:0A:E4:37:7C:E5
          inet6 addr: fe80::20a:e4ff:fe37:7ce5/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:460 (460.0 b)  TX bytes:2776 (2.7 KiB)

eth1      Link encap:Ethernet  HWaddr 00:12:F0:E9:CB:F9
          inet addr:192.168.10.100  Bcast:192.168.10.255  Mask:255.255.2
55.0
          inet6 addr: fe80::212:f0ff:fee9:cbf9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1661 errors:0 dropped:40 overruns:0 frame:0
          TX packets:1618 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1359910 (1.2 MiB)  TX bytes:376023 (367.2 KiB)
          Interrupt:11 Base address:0xe000 Memory:d0200000-d0200fff

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10040 (9.8 KiB)  TX bytes:10040 (9.8 KiB)

sit0      Link encap:IPv6-in-IPv4
```

图 9.27　确认以太网/USB 虚拟网卡已经安装

Linux 版配置工具已经解压在与 USB 驱动程序相同的目录之内，因此，首先是将它放入另一个合适的目录之内：

debian:home/carcelle/Projects/CPL/dLAN-linux-package-2.0#./configure

如图 9.28 所示，首先，我们开始为它配置编译参数。

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0
Fichier Édition Affichage Terminal Onglets Aide
dLAN-linux-package-2.0/LIESMICH
dLAN-linux-package-2.0/LISEZ-MOI
dLAN-linux-package-2.0/README
debian:/home/carcelle/Projets/CPL# clear

debian:/home/carcelle/Projets/CPL# cd dLAN-linux-package-
dLAN-linux-package-2.0/     dLAN-linux-package-3.0.tar
debian:/home/carcelle/Projets/CPL# cd dLAN-linux-package-2.0/
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
configure  install-sh  LEESMIJ  libpcap-0.8.3.tar.gz  LISEZ-MOI   README
driver     LEAME       LEGGIMI  LIESMICH              Makefile.in  tool
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ./configure
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking gcc version... 4
checking maximum warning verbosity option...  -Wall for C
checking for a BSD-compatible install... /usr/bin/install -c
checking whether ln -s works... yes
checking for modprobe... /sbin/modprobe
checking for module_prefix... /lib/modules
checking for depmod... /sbin/depmod
USB determination method: /bin/lspci -v
USB driver to be loaded: uhci
checking what kind of binaries we shall create... dynamically linked
checking for library containing gethostbyname... none required
checking for library containing socket... none required
checking for library containing putmsg... none required
checking for local pcap library... not found
```

图9.28 配置编译参数

此后，使用 make 命令（见图9.29），可以启动 PLC 配置工具的编译过程。

编译成功之后，必须使用命令 make install ，将已经编译的文件安装在合适的磁盘目录之内。

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/tool
Fichier Édition Affichage Terminal Onglets Aide
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make
making all in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/tool »
make[1]: Rien à faire pour « all ».
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/t
ool »
making all in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/driver »
make -C /lib/modules/2.6.15-1-686/build SUBDIRS=/home/carcelle/Projets/CPL/dLAN-linux
-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
  CC [M]  /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.o
  Building modules, stage 2.
  MODPOST
  CC      /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.mod.o
  LD [M]  /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.ko
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/d
river »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
config.log     driver      LEESMIJ               LIESMICH   Makefile.in   tool
config.status  install-sh  LEGGIMI               LISEZ-MOI  Makefile.old
configure      LEAME       libpcap-0.8.3.tar.gz  Makefile   README
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install
make install in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/tool »
mkdir -p /usr/local/sbin && \
        /usr/bin/install -c -m700  dlanconfig_son dlanconfig  /usr/local/sbin
mkdir -p /usr/local/man/man8 && \
        /usr/bin/install -c -m 644 dlanconfig.8.gz /usr/local/man/man8
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/t
ool »
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko
```

图9.29 编译 PLC 配置工具

在以太网/USB 虚拟网卡或以太网卡连接至 USBPLC 设备或以太网设备的情况下，使用以下命令，可以启动并运行该配置工具（见图 9.30）：

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/tool
Fichier  Édition  Affichage  Terminal  Onglets  Aide
-package-2.0/driver modules
make[2]: entrant dans le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
  CC [M]  /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.o
  Building modules, stage 2.
  MODPOST
  CC      /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.mod.o
  LD [M]  /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/driver/devolo_usb.ko
make[2]: quittant le répertoire « /usr/src/linux-headers-2.6.15-1-686 »
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/d
river »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# ls
config.log     driver       LEESMI3                 LIESMICH   Makefile.in   tool
config.status  install-sh   LEGGIMI                 LISEZ-MOI  Makefile.old
configure      LEAME        libpcap-0.8.3.tar.gz    Makefile   README
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# make install
make install in tool
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/tool »
mkdir -p /usr/local/sbin && \
        /usr/bin/install -c -m700  dlanconfig_son dlanconfig  /usr/local/sbin
mkdir -p /usr/local/man/man8 && \
        /usr/bin/install -c -m 644 dlanconfig.8.gz /usr/local/man/man8
make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/t
ool »
make install in driver
make[1]: entrant dans le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2
.0/driver »
mkdir -p /lib/modules/2.6.15-1-686/extra && /usr/bin/install -c -m 644 devolo_usb.ko
/lib/modules/2.6.15-1-686/extra
/sbin/depmod -a &&      /sbin/modprobe devolo_usb

In order to have your usb driver running and configured
at boot, you should go into driver directory and type

    make installboot

make[1]: quittant le répertoire « /home/carcelle/Projets/CPL/dLAN-linux-package-2.0/d
river »
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0#
```

图 9.30　安装 PLC 配置工具

carcelle@debian:~/Projects/CPL/dLAN-linux-package-2.0 $sudo dlanconfig eth0

该工具可以在接口 eth0 或者 dlanusb0 上运行。图 9.31 中，该配置工具正在检测已经连接到 PLC 网络 PLC 设备。

```
carcelle@debian: ~/Projets/CPL/dLAN-linux-package-2.0/tool
Fichier  Édition  Affichage  Terminal  Onglets  Aide
<-- dlanconfig software v2.0 -->


Please wait.........................
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0#
debian:/home/carcelle/Projets/CPL/dLAN-linux-package-2.0# sudo dlanconfig eth0

<-- dlanconfig software v2.0 -->


Please wait.......
Local bridge found

Local dLAN device has MAC address: 00:0B:3B:0D:D6:18

Main menu:
1) Set local network password
2) Set remote network password
3) List remote devices
4) Exit

Choose a command number: 3

Please wait.......
Local dLAN device has MAC address 00:0B:3B:0D:D6:18

Remote devices:
        Num.    MAC address          Mbps     Cache    Highspeed
        1       00:0B:3B:0B:24:15    12.829

Physical average data rate (Normal devices   )= 12.829 Mbps

Main menu:
1) Set local network password
2) Set remote network password
3) List remote devices
4) Exit

Choose a command number:
```

图 9.31　使用 Linux 版 PLC 配置工具检测以太网 PLC 设备

本例中，检测出的 PLC 设备的物理层数据传输率约为 12.829Mbit/s。由此可知，这些设备均是符合 HomePlug1.0 规范的设备。

此后，配置工具会弹出一个菜单，该菜单有如下 4 个子功能：

1）"set local network password（设置局域网密码）"：为 PLC 设备、通过以太网直接连接至该 PC 上的设备等设置 PLC 网络加密密钥（NEK）。

2）"set remote network password（设置远程网络密码）"：为连接至电力网络上的远程 PLC 设备（DEK）配置 PLC 网络密钥。

3）"list remote devices（列表查看远程设备）"：列出已经连接至 PLC 网络且配置有相同 PLC 网络密钥的所有 PLC 设备。

4）"exit（退出）"：退出该配置工具。

9.4 在 Linux 下配置 HomePlug AV PLC 网络

关于 HomePlug AV PLC 设备，对于常见的诸如 IEEE 802.11、蓝牙、IEEE 802.16（正在发布中）等的网络技术环境，合适的 Linux 工具倒不是很多。然而，有一种集成式 PLC 工具，该工具以库和包的形式发布，目前的可用包格式有 Debian 包（.deB 包）和 RedHat 包（.rpm 包）：

- FAIFA（由 Florian Fainelli、Nicolas Thill 和 Xavier Carcelle 等公司开发），其链接地址为：http://open-plc.org/。

网站 http://open-plc.org/ 收集了大量与 PLC 技术相关的信息、设备之间的兼容性以及符合 HomePlugAV 标准的固件。FAIFA 工具可以从以下地址下载。该工具的安装有多种不同方法：

- 从以下地址下载相应的压缩包，在用户所使用的 Linux 操作系统发行版上，完成项目源代码的编译工作：http://svn.open-plc.org/。

编译之前，使用以下命令，检查开发库是否存在更新：

```
#svn co http://svn.open-plc.org/
```

- 在文件 /etc/apt/sources.list 中添加以下行，以安装从 debian.open-plc.org 仓库下载的 Debian 版 faifa.deB 包：http://deb.open-plc.org。
- 安装从以下链接下载的 RedHat 包 faifa.rpm：http://rpm.open-plc.org。
- 完成 FAIFA 工具的编译与安装工作之后，就可以使用该工具的以下配置功能：
  - 配置逻辑网络 PLC 设备的网络加密密钥；
  - 检测当前逻辑网络上的已有设备；
  - 获得 PLC 设备之间链路的统计分析信息。

用户使用以下命令，可以启动 FAIFA：

```
#./faifA -i eth0  -m
```

其中，选项参数

-i：定义用来接入 PLC 网络的网络接口；

-m：打开 FAIFA 菜单显示功能选项。

FAIFA 菜单启动之后，将显示如下菜单：

```
FaifAfor HomePlug AV
Started receive thread
Supported HomePlug AV frames
type description
----  -----------
0xA000 Get Device/SW Version Request
0xA030 Get Link Statistics Request
0xA038 Network Info Request(Vendor-Specific)
0xA050 Set Encryption Key Request
0xA054 Get Manufacturing String Request
Supported HomePlug 1.0 frames
type description
----  -----------
0x0000 Channel Estimation Request
0x0004 Set Network Encryption Key Request
0x0007 Parameters and Statistics Request
0x0019 Set Local parameters Request
0x001D Set Local Overrides Request
Choose the frame type(Ctrl-Cto exit):
```

此时，可以在 HomePlugAV 和 1.0/Turbo 标准的两个子菜单中选择一个选项。如果用户选择了选项 0xA000，则工具会显示与 Intellon 芯片可用固件版本有关的信息，如下所示：

```
Choose the frame type(Ctrl-Cto exit):0xa000
Init:
Frame:Get Device/SW Version Request(0xA000)
Binary Data,60 bytes
00000000:00 B0 52 00 00 01 00 00 00 00 00 00 88 E1 00 00
00000016:A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00 00
00000032:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048:00 00 00 00 00 00 00 00 00 00 00 00
Dump:
Frame:Get Device/SW Version Confirm(A001),HomePlug-AV Version:
```

```
1.0
Status:Success
Device ID:INT6300,Version:INT6000-MAC-3-1-3103-1662-20070915-
FINAL-B,upgradeable:0
Binary Data,156 bytes
00000000:00 00 00 00 00 00 00 0CB9 08 47 0F 88 E1 00 01
00000016:A0 00 B0 52 00 02 2A49 4E 54 36 30 30 30 2D 4D
00000032:41 43 2D 33 2D 31 2D 33 31 30 33 2D 31 36 36 32
00000048:2D 32 30 30 37 30 39 31 35 2D 46 49 4E 41 4C2D
00000064:42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000096:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000112:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000128:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000144:00 00 00 00 00 00 00 00 00 00 00 00
```

用户选择了选项 0xA038 之后，FAIFA 将会发回逻辑 PLC 网络上现有其他设备的相关信息，以及符合 HomePlugAV 标准的统计信息的数量，如下所示：

```
Choose the frame type(Ctrl-Cto exit):0xa038
Init:
Frame:Network Info Request(Vendor-Specific)(0xA038)
Binary Data,60 bytes
00000000:00 B0 52 00 00 01 00 00 00 00 00 00 88 E1 00 38
00000016:A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00 00
00000032:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048:00 00 00 00 00 00 00 00 00 00 00 00
Dump:
Frame:Network Info Confirm(Vendor-Specific)(A039),HomePlug-AV
Version:1.0
Network ID(NID):B0 F2 E6 95 66 6B03
Short Network ID(SNID):0x0e
STATEI:0x01
STARole:Station
CCo MAC:
00:0C:B9:08:47:10
CCo TEI:0x03
Stations:1
Station MACTEI Bridge MACTX RX
```

```
----------- --- ---------- -- --
00:0C:B9:08:47:10 0x03 FF:FF:FF:FF:FF:FF 0x00 0x00
Binary Data,60 bytes
00000000:00 00 00 00 00 00 00 0CB9 08 47 0F 88 E1 00 39
00000016:A0 00 B0 52 01 B0 F2 E6 95 66 6B03 0E 01 00 00
00000032:0CB9 08 47 10 03 01 00 0CB9 08 47 10 03 FF FF
00000048:FF FF FF FF 00 00 00 00 00 00 00 00
```

最后一个选项为 0xA054。使用该选项，可以获得与 PLC 设备制造商的相关信息，以及网络设备间 PLC 逻辑链路的相关统计信息的数量。

```
Choose the frame type(Ctrl-Cto exit):0xa054
Init:
Frame:Get Manufacturing String Request(0xA054)
Binary Data,60 bytes
00000000:00 B0 52 00 00 01 00 00 00 00 00 00 88 E1 00 54
00000016:A0 00 B0 52 00 00 00 00 00 00 00 00 00 00 00 00
00000032:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000048:00 00 00 00 00 00 00 00 00 00 00 00
Dump:
Frame:Get Manufacturing String Confirm(A055),HomePlug-AV
Version:1.0
Status:Success
Length:64(0x40)
Manufacturer string:Intellon HomePlug AV Device
Binary Data,86 bytes
00000000:00 00 00 00 00 00 00 0CB9 08 47 0F 88 E1 00 55
00000016:A0 00 B0 52 00 40 49 6E 74 65 6C6C6F 6E 20 48
00000032:6F 6D 65 50 6C75 67 20 41 56 20 44 65 76 69 63
00000048:65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000064:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080:00 00 00 00 00 00
Dump:
Frame:Get Link Statistics Confirm(A031),HomePlug-AV
Version:1.0
Status:Success
Link ID:fc
TEI:00
Direction:Tx
MPDU acked......................:1249
```

```
MPDU collisions.................:271
MPDU failures...................:0
PBtransmitted successfully.....:1628
PBtransmitted unsuccessfully...:0
Direction:Rx
MPDU acked......................:886
MPDU failures...................:0
PBreceived successfully........:1539
PBreceived unsuccessfully......:0
Turbo Bit Errors passed.........:241
Turbo Bit Errors failed.........:0
-- Rx interval 0 --
Rx PHY rate....................:93
PBreceived successfully........:17
PBreceived failed..............:0
TBE errors over successfully....:26
TBE errors over failed..........:0
-- Rx interval 1 --
Rx PHY rate....................:93
PBreceived successfully........:15
PBreceived failed..............:0
TBE errors over successfully....:21
TBE errors over failed..........:0
-- Rx interval 2 --
Rx PHY rate....................:93
PBreceived successfully........:26
PBreceived failed..............:0
TBE errors over successfully....:47
TBE errors over failed..........:0
-- Rx interval 3 --
Rx PHY rate....................:93
PBreceived successfully........:14
PBreceived failed..............:0
TBE errors over successfully....:50
TBE errors over failed..........:0
-- Rx interval 4 --
Rx PHY rate....................:93
PBreceived successfully........:25
```

```
PBreceived failed..............:0
TBE errors over successfully....:38
TBE errors over failed..........:0
-- Rx interval 5 --
Rx PHY rate.....................:93
PBreceived successfully........:24
PBreceived failed..............:0
TBE errors over successfully....:59
TBE errors over failed..........:0
```

9.5 在 FreeBSD 下配置 PLC 网络

FreeBSD 操作系统中，可以用来配置 PLC 网络的工具极少。我们将详细讨论程序 plconfig。该程序是该类平台上当前唯一的 PLC 网络配置程序。

FreeBSD 是一种类似于 Linux 的操作系统，源自加州大学伯克利分校研发的 UNIX 内核。与 Linux 发行版相比，该操作系统存在一些不同点，基于 FreeBSD 平台进行的开发工作也略有不同。

FreeBSD 操作系统主要用于安全性较高的 Web 和电子邮件服务器。FreeBSD 使用了一种名为“ports”的包系统，用来描述该操作系统可以使用的程序。这种“ports”系统由成员遍布全球的一个开发者组织进行管理，以确保其完整性。与 Linux 相比，FreeBSD 的开发人员的数量要少得多，因此，FreeBSD 更新较慢，且一致性更好。

首先，我们从以下地址下载 Manuel Kasper 的工具程序 plconfig：https://neon1.net/prog/plconfig-0.2.tar.gz。

打开一个终端，进入终端的超级用户模式，接下来，解压缩该工具的安装程序，此后，使用命令 make 开始进行安装。如果没有将网卡或者相应的选项指定为 plconfig 命令中的参数，则该程序会显示一个帮助菜单：

```
#tar xfvz plconfig-0.2.tar.gz;cd plconfig-0.2
#make
#./plconfig
Syntax
Powerline Bridge config version 0.2 by Manuel Kasper
 <mk@ neon1.net >
Usage:plconfig [-pqrh] [-Bdevice] [-s key] interface
-s key set network encryption key
 (plaintext password or 8 hex bytes
```

```
preceded by 0x)
-Bdevice use device(default is /dev/bpf0)
-p don't switch interface to promiscuous
mode
-r request parameters and statistics
-q request Intellon-specifiCnetwork
statistics
-h display this help
If -s is not specified,plconfig will listen for
management packets indefinitely(after requesting stats if -r is
specified)
```

如该帮助菜单所示，本程序可以提供以下 PLC 网络功能：

—s：以本地方式配置通过以太网连接至该配置 PC 上的设备的 NEK。

—r：查询本地连接的 PLC 设备的 HomePlug 芯片的相关信息，也可以获得参数和统计信息的数量。使用该选项，还可以显示电力网络上配置正确的 PLC 设备。

—q：查询 PLC 芯片的信息，以及获得与 Intellon 芯片生产商有关的数据和统计信息。

从以上叙述可知，该程序的功能比 Windows 或 Linux 平台的相关工具要少，但是，还是拥有配置 PLC 网络所必需的主要功能（配置网络密钥、查询物理层 PLC 链路的状态信息等）。

9.6 配置 HD-PLC 网络

HD-PLC 由松下公司制定。该公司主要按照标准 BL-PA300（PL-HNC-006）P/N 向日本市场推出工作电压为 110V/50～60Hz 的 HD-PLC 设备。HD-PLC 标准适用于主-从模式的网络。这类网络中，有一个网络设备工作于主模式（通过设备上的按钮设置），其他的设备则工作于从模式（也是通过设备上的按钮进行设置）。HD-PLC 设备上的嵌入式软件（基于 ARM926-EJS 硬件架构和 μITRON OS，且符合 PX-PRP1A9-4 参考标准）有 3 个主要组件：

1）IP 栈和 HTTPD：使用 HD-PLC 设备的嵌入式 Web 界面可以完成设备的配置。

2）DataLink 栈：用于管理 PLC 接口、以太网接口和串行接口。

3）任务通信栈：与用于任务通信、中断处理程序和缓冲器等的邮件和事件配合使用，目的是实现与硬件接口的信息交换。

9.7 配置 DS2 网络

西班牙的制造商 DS2 是 HomePlug 市场的供应商之一，但是，它们的产品却不

兼容 HomePlug 设备。

DS2 200Mbit/sPLC 网络通过 HTTP 接口在设备上以本地方式进行配置。因此，对于 Windows 和 Linux/FreeBSD，其配置过程完全相同。

DS2 设备可以工作于 3 种不同的网络模式：

1）HE：PLC 网络的主设备。

2）CPE：PLC 网络的从设备。

3）TDREP：PLC 网络的中继器。

本章中，我们将详述基于 DS2 Wisconsin 芯片的 Corinex AVPLC 设备。这类设备中，有两种类型的固件：almA 和 spirit。我们选用使用 almA 固件的设备，因为这类设备的功能更强。

在连接至 HTTP 接口之前，必须将 PLC 设备和配置用 PC 的 IP 地址设置在同一个网段。Corinex AV PLC 设备的默认 IP 地址为 10. 10. 1. 69，因此，配置用 PC 的 IP 地址必须设置为该 IP 地址同一网段的地址，例如 10. 10. 1. 10。图 9. 32 描述了同一电力网络上存在不同子网地址的情况。连接上主页之后，输入默认密码（paterna），可以打开配置页面（见图 9. 33）。

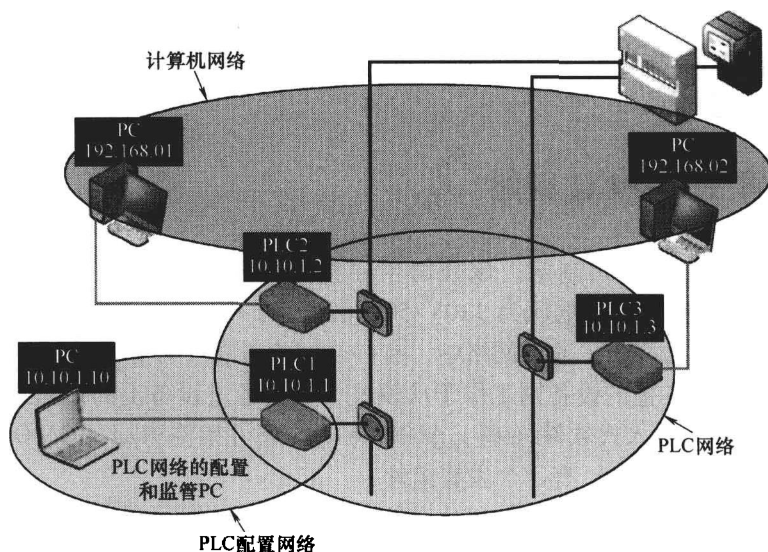


图 9. 32 DS2PLC 网络的寻址网段

第一个配置页简要列出 DS2PLC 设备的主要参数（见图 9. 34），其中，重要的有：

1）PLC 设备的 IP 地址；

2）PLC 设备的 MAC 网络模式（HE、CPE、TDREP）；

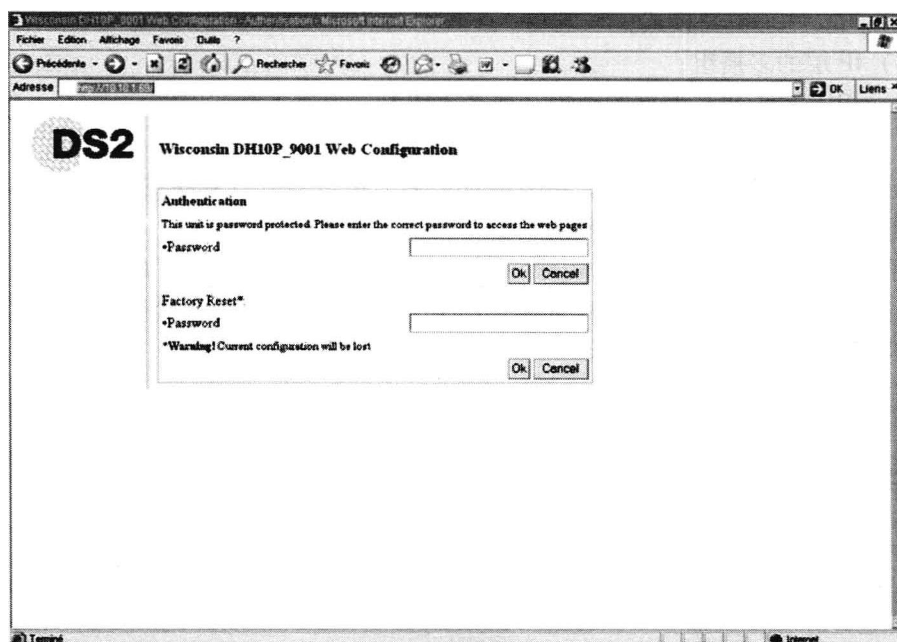


图 9.33　DS2 配置工具的 HTTP 主页

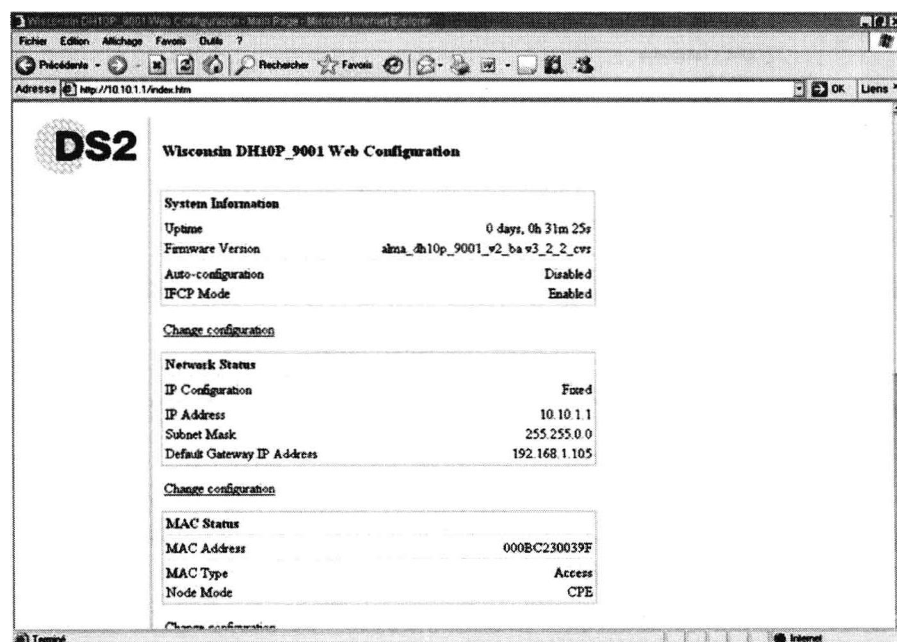


图 9.34　DS2PLC 设备的配置参数

3）PLC 物理链路模式；

4）IP 层的多播组；

5）用于保证 PLC 网络的密钥（或者密码）；

6）PLC 设备之间某些数据流的优先级。

这些参数可以单独地配置，经过验证之后，可以写入计算机的永久性存储器。对配置进行全面更改之后，重新启动设备，新配置才会发生作用。

单击“Default GatewayIPAddress（默认网关的 IP 地址）”之下的“Change configuration（更改配置）”，可以配置设备的 IP 地址、子网掩码和默认网关等。此时显示的配置页面如图 9.35 所示。

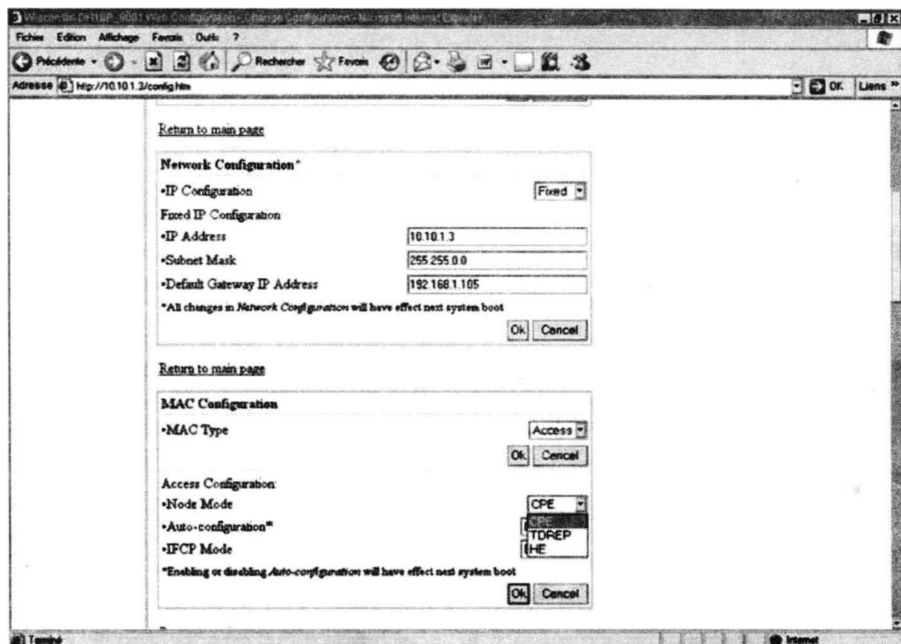


图 9.35　DS2PLC 设备 MAC 地址和网络参数的配置

在图 9.36 的示例中，设备 PLC1、PLC2 和 PLC3 的地址分别为 10.10.1.1、10.10.1.2 和 10.10.1.3，子网掩码则为 255.255.0.0。这种情况下，默认网关无关紧要，因为，配置用 PC 的地址已经处于同一个网段之内（10.10.1.10）。

完成这些网络参数的配置之后，必须配置每一个 PLC 设备的网络模式。

如图 9.36 所示，最接近断路器面板的设备配置为主（HE）模式，而其他的设备则被配置为从（CPE）模式或者中继器（TDREP）模式。设备之间的电力线过长使得信号不易于抵达目标设备或者因楼宇限制难以抵达其他电力环境时，可以使用中断器模式。

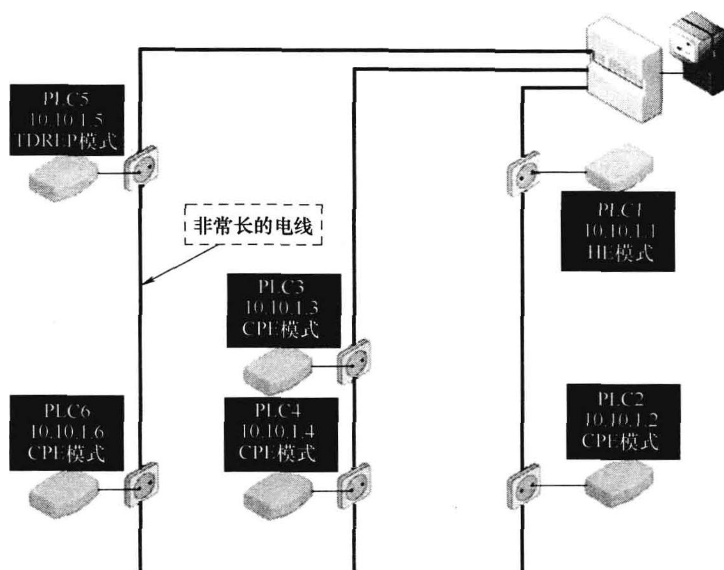


图 9.36 配置 DS2 PLC 设备的网络模式

在 MAC 配置窗口面板的访问配置区，选择节点模式，可以完成该项配置。此时，会弹出一个窗口，从中可以选择 3 种模式中的任意一种。

可以为 DS2 PLC 设备创建多播 IP 组类型，此后，IP 帧从源设备出发，可以发送至属于同一个多播组的多个目标设备。创建"多播" IP 组，必须熟悉掌握 IP 网络的配置技术（参见本章尾部）。

对于任何类型的 PLC 网络，其中一个关键参数就是网络密钥。DS2 配置工具中，将其称之为"密码"；使用该参数，可以创建私有 PLC 网络，确保网络组件（连接至 PLC 网络的设备和终端）之间的数据交换安全。在"Security Configuration（安全配置）"区（见图 9.37），输入该网络特定的 PLC 网络密码，可以完成该项配置。该参数相当于 HomePlug PLC 网络中的网络加密密钥（NEK）。

此后，根据网络拓扑和各个设备的功能，在"Priority configuration（优先级配置）"区将参数"Default priority（默认优先级）"设置为 1 ~5 中的某个数值，就可以完成每个网络 PLC 设备的优先级配置。

例如，针对图 9.37 中的网络拓扑，可以为主模式设备配置较高的优先级（值 1），而将某些 CPE 模式的 PLC 设备（如果它们所连接的终端上部署有实时应用的话），设置"average（中等）"优先级（值 2）。其他设备均可以配置为"low（低）"优先级（值 3 或 4）。

在图 9.38 所示的 HTML 网页上，可以访问 PLC 网络的安全配置参数（配置界

面密码、PLC 网络 ID、工厂复位密码等）和 PLC 网络上各设备的优先级配置参数，尤其是参数“Default priority（默认优先级）”。

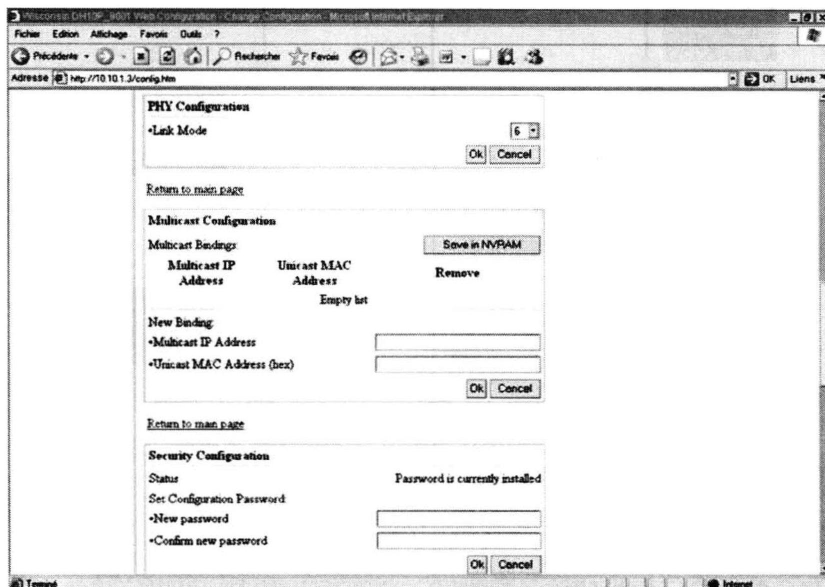


图 9.37　DS2 PLC 设备的物理层参数、多播组参数和安全参数等的配置

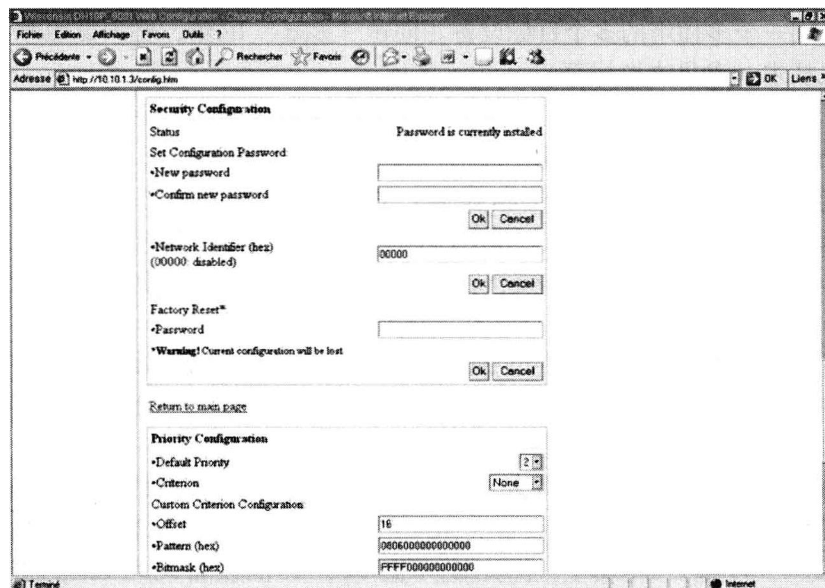


图 9.38　DS2 PLC 设备的优先级和安全参数的配置

通过端口40000上的Telnet终端，使用以下命令，也可以配置DS2PLC网络：

```
C:\>telnet adresseIP_equipement_CPL 40000.
```

adresseIP_equipement_CPL 为分配给通过以太网接口连接至配置用PC上的PLC设备的IP地址。

通过Telnet终端进行配置，还可以使用一些高级功能，例如查看PLC设备的温度、为某些频段开槽、PLC网络之间的桥接和漫游功能等。

9.8 配置网络参数

为了完成PLC网络的配置，还必须为各个设备分配正确的网络参数，这些参数包括IP地址、子网掩码、默认网关地址、DNS地址等。

进行实际的配置工作之前，以下章节首先回顾了管理诸如IP地址、子网掩码、DNS地址等网络配置信息时所必须注意的事项。

9.8.1 网络参数回顾

网络通信管理由与所用标准有关的大量功能决定。这些功能中，有一个是因特网协议（IP）。IP定义如何与寻址系统和特定的路由机制进行通信。

IP地址

连接至局域网或因特网的每一台计算机，均组合使用了两个协议，即TCP（或UDP）和IP，其更常见的表现形式为TCP/IP或UDP/IP。为了实现通信，每台计算机均持有一个唯一的IP地址。IP地址的形式为x.x.x.x，其中，x表示0~255之间某个数字。

IP有两个版本：IPv4和IPv6。目前，最常见的为IPv4地址。该地址长4B，仅能支持有限的功能（主要是路由功能）。IPv6则是IPv4的升级，但很少用于目前的网络。其地址长16B，可以提供大量功能，诸如移动性、服务质量和安全管理功能等。

IPv4地址的结构

IPv4地址长为4B，即32bit（1B为8bit）。

每个IP地址均有两个部分：

1） 网络地址；

2） 与计算机地址对应的主机编号。

假设有一个网络由3台计算机组成，这3台计算机的地址分别为145.41.12.1、145.41.12.2和145.41.12.3。这种情况下，网络地址为145.41.12.x；1、2和3则对应于各计算机的主机地址。

在这种寻址方案下，该网络可以连接的计算机的地址范围为145.41.12.1～

145.41.12.254。145.41.12.255为保留地址，为“广播地址”，用于将信息发送给网络内的所有工作站。在网络连接性方面，这类寻址方案的能力较差，因为，它仅能寻址254个计算机。

视网络地址容量的不同，网络的数量以及互联主机的数量都可以不同。考虑到这种差别，人们定义了地址类别。

地址类别

IPv4定义了5种地址类别，见表9.4。

表9.4 IPv4的地址类别

地址类别	地址范围	网络的数量	单个网络内的主机数量
A类	1.0.0.0~126.0.0.0	126	16777214
B类	128.0.0.0~191.255.0.0	16384	65534
C类	192.0.0.0~223.255.255.0	2097152	254
D类	224.0.0.0~225.0.0.0	组地址（多播地址）	
E类	225.0.0.0~240.0.0.0	实验用	

这些地址类别的定义主要是根据网络地址所使用的字节数量：

1）对于A类地址，第1个字节（8bit）专门提供给网络地址使用，且该字节的第一位设置为0。因此，A类地址所包含的网络地址的范围为0000000~0111111（二进制格式）。考虑到地址0.0.0.0和127.0.0.0被保留，因此，可以使用的A类网络地址共有2^7-2，即126个，范围为1.0.0.0~126.0.0.0。

主机的数量由3个字节（24bit）确定。由于广播地址（x.x.x.255）和地址x.x.x.0被保留，所以，每个A类网络地址可以容纳的主机数量为$2^{24}-2$，即16777214个。

2）对于B类地址，前2个字节（16bit）专供网络地址使用，且其前两个位分别被设置为1和0。因此，可用B类网络地址的总数量为$2^{14}-2$，即16384个，范围为128.0.0.0~191.255.0.0。

每个网络地址可以容纳的主机数量由两个字节确定。与A类地址相似，广播地址和x.x.x.0地址被保留它用，因此，单个B类网络地址可以容纳的主机数量为$2^{16}-2$，即65534个。

3）对于C类地址，前3个字节（24bit）专供网络地址使用，且其前3位分别设置为1、1和0，因此，可以使用的C网络地址共有$2^{21}-2$，即2097152个，范围为192.0.0.0~223.255.255.0。

主机的数量由1个字节（8bit）确定。类似地，由于广播地址和地址x.x.x.0被保留，所以，每个C类网络地址可以容纳的主机数量为2^8-2，即254个。

C类和D类地址均保留，供实验性组播寻址使用。

IP地址并不是自动分配，且并非所有任意一个地址范围都可以分配给某个网

络。因特网分址机构（IANA）负责为申请者分配这些地址。然而，必须注意，所有可用A类和B类地址均已经分配完毕。

IP地址是可路由地址，这意味着这些地址不得用于私人目的。

为了避免使用不正确的IP寻址，IANA保留了以下3个地址范围，供严格限制的3类私人使用目的：

1）A类：10.0.0.1～10.255.255.254；

2）B类：172.16.0.1～172.63.255.254；

3）C类：192.168.0.0～192.168.255.254。

为了连接至因特网或者连接至使用了不同寻址方案的网络，拥有私有IP地址的各个工作站均必须指定一个默认的网关地址。该地址对应于负责处理网络路由的某个站，用于处理从非路由环境（私有网络）至可路由环境（因特网）的发送请求和接收请求。

通过网关共享因特网连接时，网关负责将请求从私有环境（因而也是非路由环境）发送至因特网环境（可路由环境）。这种情况下，默认网关地址即为网关的IP地址。

子网掩码

掩码用于与计算机的IP地址进行二进制减法运算，从而获得计算机的网络地址。

若某个计算机的IP地址为192.168.0.1，掩码为255.255.255.0，将这两个地址做二进制减法运算，结果为192.0.0.0，该值即为网络地址。

通常，A类、B类和C类地址的掩码分别为255.0.0.0、255.255.0.0和255.255.255.0。

在配置两个计算机的掩码时，如果其中一台计算机的IP地址为192.168.1.1、掩码为255.255.255.0，另一台计算机的IP地址为192.168.1.10，掩码为255.225.0.0，则它们的网络地址（192.168.0.x和192.168.1.x）不相同。因此，它们不属于同一个网络，不能相互通信。

DNS（域名服务）

DNS使用了一种分层结构，由一组服务器组成。使用DNS，可以将IP地址和域名关联起来。域名则由机构名和级别（例如.fr、.com等）组成。

相对IP地址而言，使用域名可以更加容易地记住网站地址、电子邮件地址或者FTP地址。

使用域名也可以获得某个特定的服务器或者网站的IP地址。

通常，在配置网络参数时，需要设置两个DNS服务器地址。这样，当一个服务器故障时，还可以正常地访问网络。DNS地址是必不可少的IP地址。

9.8.2 在WindowsXP环境中配置网络参数

在控制面板中，选择“Network（网络）”。此后，在网络组件区，选择您的

Wi-Fi 网卡的 TCP/IP 组件，并单击“Properties（属性）”，打开属性对话框。

将您的因特网服务提供商提供的信息，按需填入各个字段：

1）IP 地址，对应于计算机的 IP 地址；

2）子网掩码，用于获得上面的 IP 地址的网络地址和子网地址；

3）默认网关，对应于连接至因特网的网络计算机的地址；

4）DNS 地址，通常由 IAP 或者网络管理员提供。

如果使用了 Windows2000 和 XP 以外的其他 Windows 版本，则必须重新启动计算机。

对于 Windows2000 或者 XP，最多需 10s，用户定义的网络参数就会起作用。

9.8.3 在 Linux/BSD 环境中配置网络参数

为了配置网卡的 IP 地址和子网掩码，在 shell 终端中输入

```
# ifconfig eth0 10.0.0.2netmask 255.255.255.0
```

需要配置网关地址（该例中为 10.0.0.1）时，输入

```
# route add default gw 10.0.0.1
```

使用 route 指令，可以检测路由表中是否已经添加了该网关地址：

```
# route
    # route
    Kernel IP Routing Table
    Destination  Gateway  Genmask  Flags  MetriCRef
    Use Iface
    Default    10.0.0.1 0.0.0.0    UG    0    0
    0 eth0
```

为了配置域名服务器的地址，可以使用 vi 命令，打开目录/etc 的 resolv. conf 文件：

```
# vi /etc/resolv.conf
```

以下为一个 resolv. conf 文件示例：

```
nameserver adresse_IP_DNS
domain nom_de_domaine
```

nameserver 用来定义首选 DNS 地址，domain 则用于定义网络域名（如果有的话）。类似于 DNS 地址，域名由 IAP 提供。如果拥有多个 DNS 地址，对于每个备用的 DNS 地址，仅需要添加一个 nameserver adress_IP_DNS 行。

如果网卡为 PCMCIA、PCI 和 Mini-PCI 卡，则通过对文件 /etc/pcmcia/network. opts（对应于 PCMCIA 卡）和文件 /etc/network/interfaces（对应于后两种卡）进行配置，也可以以半自动方式完成该项配置。

第10章　PLC在家庭中的应用

尽管PLC设备的价格偏高，但越来越多的人尝试着在家中安装PLC网络。做出这种选择的主要原因是不需要另外单独布设电缆。

实际上，在家中安装PLC网络确实非常简单。您所要做的就是将PLC设备连接到家中的电源线上并且配置一下。理想情况下，家中应该有一个ADSL调制解调器（电缆式的、卫星式的，甚至是56k普通拨号式的）可供接入因特网，接下来只需将ADSL连接到PLC设备上。这时PLC设备起到了网关的作用，即可为家中所有电力插座提供因特网接入服务。

运营商目前提供了新的因特网接入方式，这两种方式都是通过“盒子”实现的：一种是将ADSL调制解调器连接在电话接线盒上；另一种是连接在视频解码盒上，它从因特网接收视频数据流，并将其播放到普通电视或数字高清晰电视屏幕上。一些因特网接入服务商（IAP）引入两种PLC设备，从而将ADSL调制解调器和视频解码盒连接起来。这一技术趋势将随着家庭用户的基于IP业务的HD（高清晰）视频业务的不断发展而更加明朗。HD Over IP将用作向家中的不同电视广播视频数据流。就吞吐率和信号覆盖效果而言，PLC设备是播放这些IP数据流的最佳方案之一。

PLC家庭网络拓扑结构取决于不同的需求和电力网络的结构，也取决于所采用的设备和网络运作方式。

如图10.1所示，在PLC家庭网络中，PLC设备通过调制解调器连接至因特网，从而实现了连接的共享。

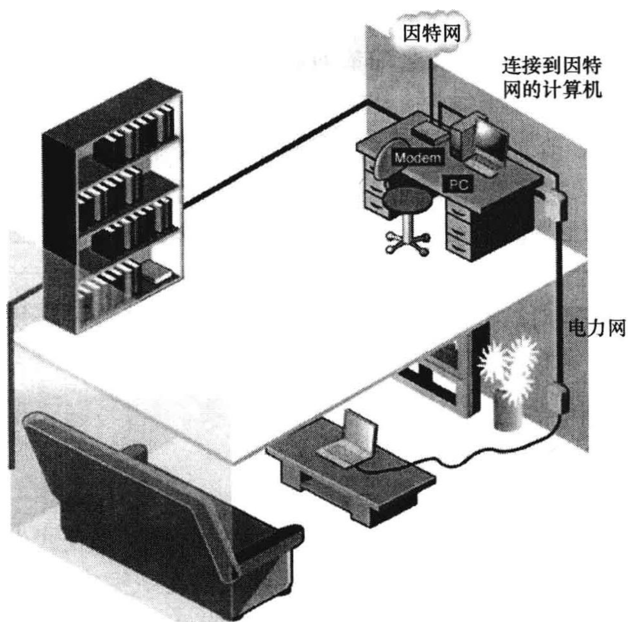


图10.1　PLC家庭网络共享因特网连接

本章主要介绍PLC家庭网络的优化安装，从设备的选择一直说到安装和配置环节。安装家庭PLC网络并不是一件难事，但是一定要遵守一些规则，尤其是关于电力网和安全操作方面的规则。

10.1 电力安全

PLC技术的媒介是110或220V/50或60Hz低压电力网络。考虑到这种电力网络可能危及人类安全，因此为了避免触电事故，遵守一些基本的安全法则是非常重要的。

图10.2就是一个典型的有电危险的标识。

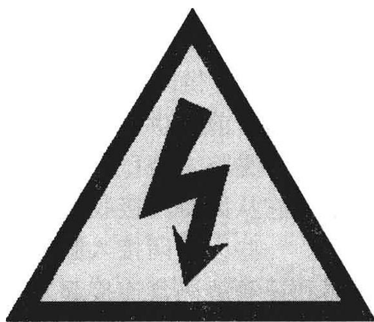


图10.2 有电危险的标识

我们必须遵守如下主要的电气安全规则：

1）安装一个500mA差模电路断路器以防短路；

2）使用电路断路器或者不超过16A的熔丝保护插座；

3）请勿将设备暴露在阳光下或者靠近热源；

4）请勿用洗涤剂或气溶胶清洗电气设备；

5）在切断电源之前请勿拆开电气设备，并且在断电几分钟之后，再进行拆卸；

6）请勿将设备安装在水源附近（浴缸、淋浴头、洗衣机、游泳池等）；

7）为了防止电线起火，请勿使用过长的电源延长线和过载电源盘；

8）请按照电气设备的操作说明操作设备；

9）在没有电工的帮助时请勿尝试在电力线上安装PLC插座。

如果对这些规则或者对准备安装PLC网络的环境有疑问，建议与专业电工或PLC专家联系。

10.2 选择PLC技术

如前面几章所述，目前IEEE1901标准还未正式生效，在PLC领域中有着为数不多的技术和标准规范。尽管这些规范在一些功能方面有共性，但是它们依然有着诸多不同。只有HomePlug联盟的规范可看作一种事实标准，因为市场上大部分PLC设备都符合这个规范。

表10.1总结了当前可用的各种PLC技术的标准。

表 10.1　PLC 技术选择参数

PLC 技术		首选用途和应用场合
HomePlug	1.0TurboAV	家庭网络工作，因特网广播，IP 视频流（HomePlug AV），音频广播
	Oxance	专业网络，工业应用，提升服务质量
	BPL	PLC 用于本地的中压电力网络
DS2		专业网络，高速率家庭网络 （声音，数据，高精确度 IP 音频）
Spidcom		专业网络，工业应用，自动 PLC
Main. net		PLC 用于本地的中压电力网络

10.3　选择设备

自符合当前各类通信吞吐率需求的 HomePlug Turbo 产品问世以来，HomePlug 1.0 的产品价格就大幅度下跌。接着，HomePlug AV 设备的出现又导致了 HomePlug 1.0 和 Turbo 设备的价格下跌。

为了满足当前通信应用的需求（在房间中广播 IPTV、数据和因特网语音数据流），HomePlug AV 设备似乎正好符合家庭用户对最佳性价比的期望。

家庭网络设备（网络游戏、接收或者显示平台与媒体节点之间的语音、数据和视频流的广播）终端之间的吞吐率需求不断上升，再加上家庭网络设备往往需要接收各地网络接入供应商的服务，因此需要家庭网络设备的吞吐率在物理层达到大概 200Mbit/s，而这正是 HomePlug AV 所能做到的。

目前，HomePlug 的所有设备都可兼容 1.0 和 Turbo 系统。尽管如此，不同的 HomePlug 产品用于不同应用场景的情况仍将维持一段时间，例如：

1）HomePlug1.0：Web 浏览器、电子邮件；

2）HomePlug Turbo：因特网、IP 电话、数据（大规模数据交换）、图像（IPTV 、MPEG-2 或 MPEG-4）；

3）HomePlug AV：基于 IP 格式（比如 MPEG-2）的数字高清视频在不同显示终端播放。

10.4　电力网络中的设备安装

为了获得良好的网络质量和实现网络数据流（语音、数据和 IPTV）的广播，

根据下列规则，在电网上尽可能有效地安装 PLC 设备就显得非常重要。

1）电力网络的拓扑结构；

2）IP 终端的位置以及连接因特网调制解调器 PC 可能的位置。

安装 PLC 设备的理想位置如下：

1）靠近电路断路器面板的附件（这里是各个插座、电器设备和电灯的电力线路起始的地方）；

2）靠近连接到电信交换网络因特网调制解调器的（语音接线盒）上。

图 10.3 是一个常规的家庭因特网接入布线示意图。PLC 设备安装在整个房间连接到因特网的电话接线盒附近的插座上。

图 10.3　家庭中常规的因特网接入布线示意图

这种安装中，采用 3 个设备来确保 PLC 设备能够接收到因特网数据流并且覆盖良好：

1）PLC 网关设备连接到以太网（电话线）调制解调器接线盒，并连接到插座 1 上；

2）向固定的 PC（例如插座 3）提供网络服务的 PLC 设备可连接到上一线路上。

3）服务便携 PC（插座 5 和 6）的设备可安装在不同的楼层以提供家庭中的移动性。

这种配置有 3 种 PLC 设备的网络在家用环境中应用最为广泛。越来越多的家庭至少拥有两台电脑和一个高速因特网接线盒。

图 10.4 是在图 10.3 基础上连接了各种具体设备的示意图。安装了这些设备后，就可以将不同的因特网信息流传播到电力网的插座上去。

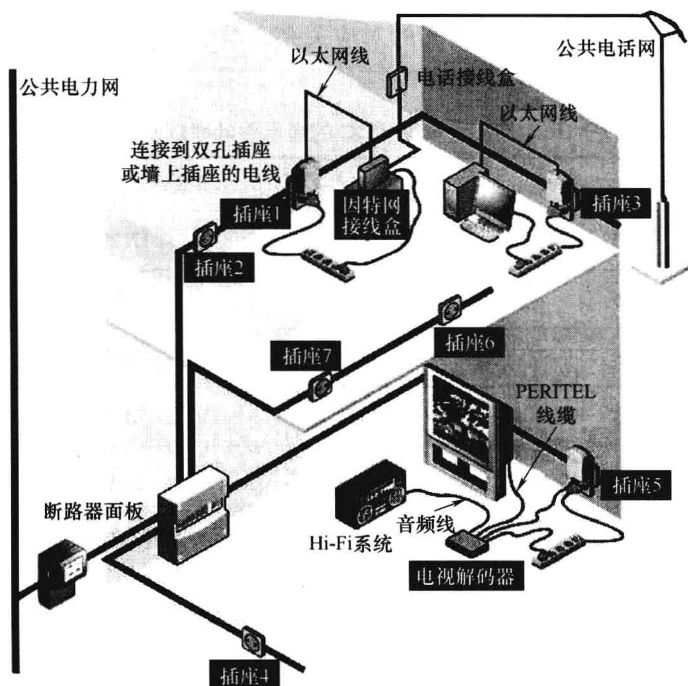


图 10.4　家庭网络的各种设备安装示意图

位于插座 3 旁的 PLC 设备是供 PC 使用的。PC 可以通过插座（插座 1 ~ 插座 3）连接到因特网。显然，重要的是寻找到一种令人满意的折中方案，一方面需要达到设计的数据吞吐率，另一方面就是为了确保 PLC 网络连接的质量，要确定 PC 连接在插座 3 上，还是连到插座 2 或插座 1 上。

如果使用的是 HomePlug Turbo 设备，就可以使用一个 PLC 配置工具（比如第 9 章中所述的智能电力包单元），在一个插座上实现吞吐率为 12 ~ 75Mbit/s 之间的网络连接。对同一楼层相邻房间的其他插座而言，基本上也是这个水平。

位于插座 5 上的 PLC 设备为电视信号解调提供数据流，通过这个 PLC 设备连接到因特网接线盒上，重新呈现来自因特网的视频数据。为了保证流畅

的电视效果，这些视频信息流需要至少 1Mbit/s 的稳定有效的吞吐率。不能让电力线网络上的视频信号质量降低太多，以至于图像不能显示，这一点很重要。这些约束条件意味着插座 5 和插座 1 之间的 PLC 通信链路能提供 1.5Mbit/s 的有用吞吐率。这个吞吐率一般能够通过 PLC 配置工具来检测。所提到 PLC 设备必须直接插到墙上的插座孔或者是两用并排插座的插孔中，而不是配电盘上。

表 10.2 列出了 HomePlug Turbo 设备在配置工具上显示的吞吐率和基于 PLC 网络的 IP 网络应用的有效吞吐率之间的对应关系。根据这张表，我们可以发现，插座 5 至少具有 10Mbit/s 的显示吞吐率才行[⊖]。

表 10.2 HomePlug Turbo PLC 的显示吞吐率以及有效吞吐率

显示吞吐率/(Mbit/s)	有效吞吐率/(Mbit/s)
85	12.23.5
75	11.8
55	9.42
45	8.79
3	8
25	7
14	4.5
12.83	3.5
11	3.2
10.16	2.9
8.36	2.4
6.35	2
4.04	1.22

⊖ 作者前文提到为了保证流畅的电视效果，需要至少 1Mbit/s 的稳定有效的吞吐率。为了不让电力线网络上的视频信号质量降低太多，需要插座 5 和插座 1 之间的 PLC 能有 1.5Mbit/s 的有效吞吐率。累加起来，有效吞吐率需要至少 2.5Mbit/s，对应表 10.2 可查到显示吞吐率应大致为最低 10Mbit/s。——译者注

（续）

显示吞吐率/(Mbit/s)	有效吞吐率/(Mbit/s)
3	0.89
1	0.33
0.9（RORO 模式）	0.2

那些来自因特网的模拟语音信号流以及在电话接线盒的 RJ-11 连接器上的模拟语音信号流也可以通过电力网络来进行广播。

与 HomePlug PLC 设备不同，Niroda 公司的 Wingoline 设备可根据不同的私有通信协议提供 3.3～8.2MHz 的带宽。因此，由 Niroda 公司的设备组建的 PLC 网络，不能与 HomePlug PLC 网络互联。通过增加一根电话线，在同一个电力网络中最多可以配置 24 个 Niroda 公司的 PLC 设备。

图 10.5 展示了在下列 PLC 网络中，通过 IAP 提供的因特网可以实现的网络连接：

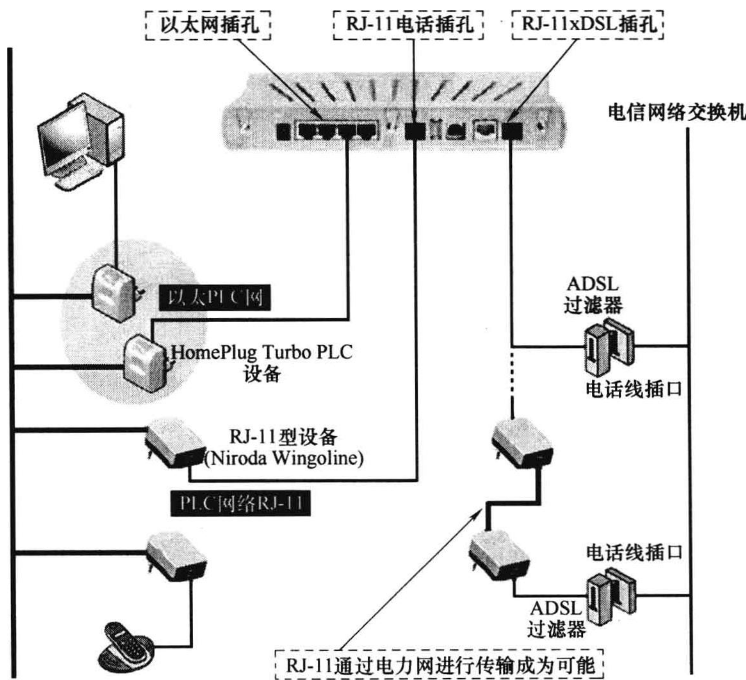


图 10.5　多种 PLC 网络连接到一个因特网接线盒的示意图

1）用于连接房中 IP 终端到因特网接线盒的 HomePlug 以太网 PLC 网络；

2）用于连接模拟电话设备和因特网语音线路插孔的 RJ-11 PLC 网络；

3）通过家庭电力线路将因特网接线盒与电信运营商 xDSL 上网设备相连接的 RJ-11 接口 PLC 网络。

下列 RJ-11 PLC 网络的 Niroda 公司的设备能够像图 10.6 所示的那样安装：

1）因特网接线盒通过 RJ-11 电话插孔，连接到电力网络的插座 1 上；

2）电话 1 通过 Niroda 公司的设备，连接到电话 PLC 网络上的插座 3 上；

3）用同样方式将 2 号电话机连接到插座 5 上。

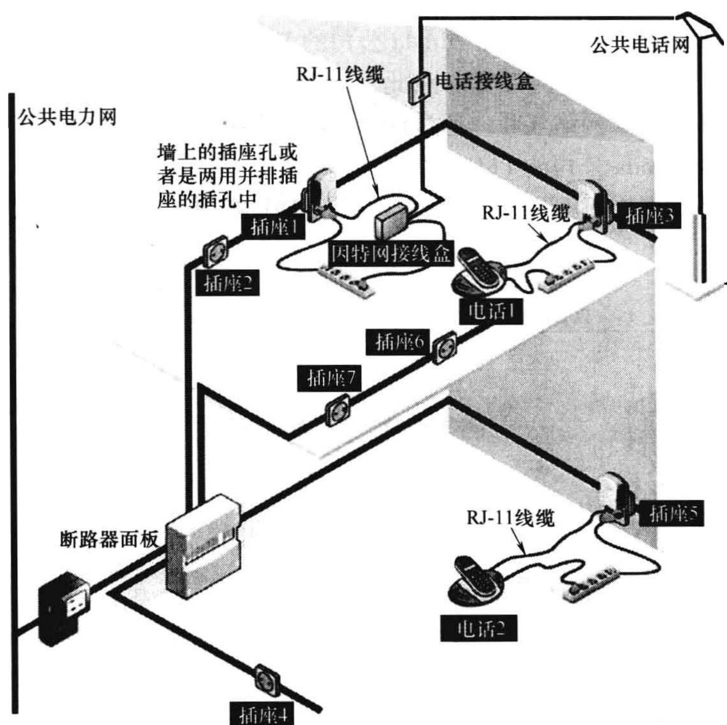


图 10.6 基于家庭电力网的 IP 电话分布示意图

由于电话通信技术需要 20kbit/s 的吞吐率，因此在中等规模的家庭中（一般有 3～4 个房间）实现上述电力线应用是很可能实现的。

图 10.7 给出了在家用电力线网和电话线网上往复着的信号和信息流的情况：

1）电话机和因特网接线盒 RJ-11 接口之间的模拟语音信号；

2）来自 ADSL 的因特网 IP 数据流。

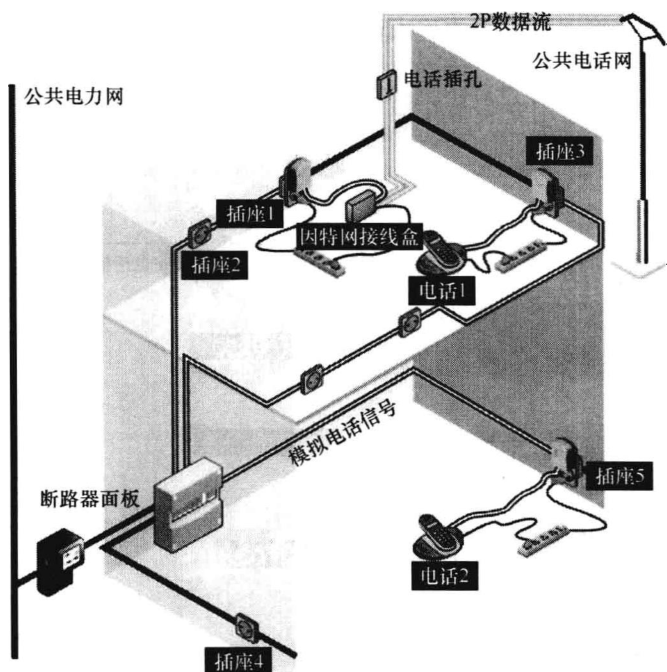


图 10.7　在家庭电力网络上广播模拟电话信号

10.5　配置安全参数

即便在家庭中，PLC 网络的保护也是一个很主要的环节。利用电力线来进行组网，就意味着网络覆盖区域或多或少地会外延到家庭以外。这就致使任何人都可能会接入到这个电力线网络，从而进入因特网。

PLC 网络提供安全机制，用合适的密码管理方案来防止窃听。

为了用一种更可靠的方式来保护网络，还有其他防火墙解决方案可供使用（鉴权服务器和虚拟专用网络）。

10.5.1　配置 PLC 网关

网关概念好像有些不容易理清楚，因为在同一个网络中存在着以下几种因素所定义的网关：

1）因特网、调制解调器或者因特网接线盒网关，一般是以 xDSL 方式通过电话线插孔将房子连入因特网；

2）以太网网关，将调制解调器、路由器或者因特网调制解调器连入本地局域网络，配置网络安全参数（本书后续章节详细介绍）；

3）PLC 网关，将因特网网关连入电力线网络，将来自因特网的 IP 流转发到电力网中。

图 10.8 说明了在家用安装中几种不同网关类型的位置。

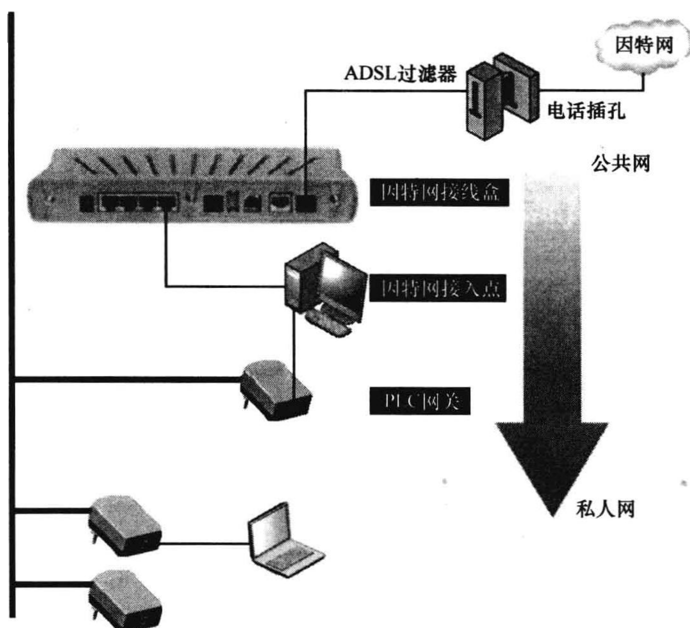


图 10.8　私人网连接到公众网上时的不同网关位置示意图

相比网络中的其他 PLC 设备，由于 HomePlug Turbo 设备是按照点对点模式工作的，因此对于 HomePlug 设备而言，PLC 网关不需要特殊的设置。PLC 网关的这种特殊性质是由于该设备被连接到因特网网关，而且所有流向因特网的 IP 数据流都经过了这个设备。

唯一需要 HomePlug 特殊定义的 PLC 网关参数就是优先级（参数 CA0、CA1、CA2 和 CA3 定义了 4 个优先级）。表 10.3 总结了 HomePlug 中这 4 个优先级的特征。

表 10.3　PLC 网关的数据业务分级

<table>
<tr><th>数据业务分级</th><th colspan="2">HomePlug1.0 和 Turbo 优先级</th></tr>
<tr><td>0</td><td rowspan="2">CA0</td><td rowspan="4">低优先级</td></tr>
<tr><td>1</td></tr>
<tr><td>2</td><td rowspan="2">CA1</td></tr>
<tr><td>3</td></tr>
</table>

（续）

<table>
<tr><th>数据业务分级</th><th colspan="2">HomePlug1.0 和 Turbo 优先级</th></tr>
<tr><td>4</td><td rowspan="2">CA2</td><td rowspan="4">高优先级</td></tr>
<tr><td>5</td></tr>
<tr><td>6</td><td rowspan="2">CA3</td></tr>
<tr><td>7（最高优先级）</td></tr>
</table>

这种分级方式继承了 IEEE. 802. 1D 标准等级的描述，并且将 IEEE802. 1D 协议中的 8 组优先等级系列简化成 PLC 网络中的 4 个优先级。

在 PLC 网关中配置 CA 优先级的参数值，最简单的方法就是设置 CA3 的参数，允许经过那些可能成为 PLC 网络瓶颈的设备优先输入或者输出数据流量。

目前 PLC 配置工具还不能用于配置这些参数，因此，开发了一种专门基于 Windows 操作系统的特殊工具，该工具以可执行文件开始。这个程序可以在以下网址下载：http://carcelle. fu8. com/ConfigureationPrioriteCPL. zip。

在以太网网卡上用 WinPCap 工具管理网络上输入输出数据的，必须事先安装好此工具。这个工具一般会随 PLC 配置工具事先预安装，如果没有，可以在下面这个网址下载：http://www. winpcap. org/inatall/bin/WinPcap_3_1. exe。

一旦下载并安装好 WinPCap 工具，就可以按下列方法开始安装 ConfigurationPrioritéCPL 工具。

1）下载 ConfigurationPrioritéCPL. zip 文件，然后解压缩到本地文件夹；

2）双击 ConfigurationPrioritéCPL. exe 文件运行。

这个工具软件安装成功后，Window 虚拟 DOS 界面将会如图 10.9 所示的那样提示您选择一种优先级：0（CA0）、1（CA1）、2（CA2）或 3（CA3）。



图 10.9　PLC 优先级配置工具启动示意图

选好优先级后，这个软件提示您选择当前 PC 上连接到 PLC 设备的以太网网卡。IP 地址信息用于识别当前网卡。在图 10.10 的例子中，与 PLC 网关相连的是 3 号网卡，其 IP 地址是 192.168.0.10。

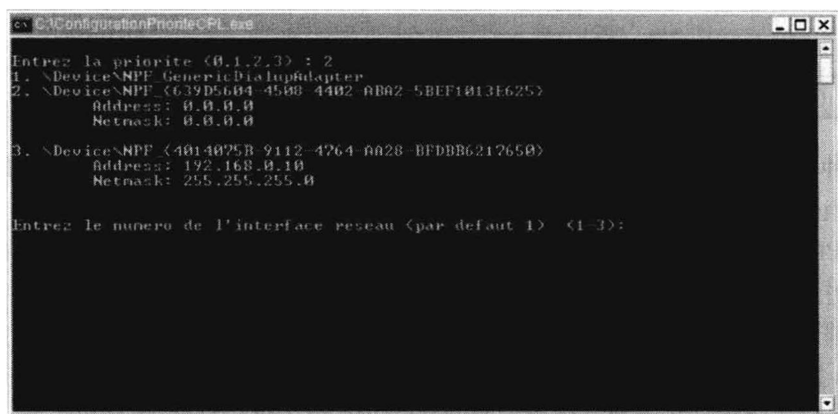


图 10.10 配置连接到 PLC 设备上的网卡示意图

选好网卡后，Window 虚拟 DOS 界面会自动关闭，这意味着优先级配置完成。

重要的是，要确认 PLC 设备的优先级已设定为最高，并且保证它连接到因特网网关或因特网接线盒。

10.5.2 配置 PLC 安全参数

PLC 安全参数的配置，是 PLC 网络保证网络内部之间安全交换数据的要点。由于 PLC 信号会传播到家庭电能表范围以外，如果 PLC 设备仅仅只是按照 NEK 的默认参数进行配置，任何不轨之人都可以截获数据。

在相互连接的 HomePlug 设备中配置不同的 NEK 安全参数，多个 PLC 网络也可以安装在同一个电力线网络中，并且还都带有安全防护措施。

如第 9 章所述，为了配置 HomePlug PLC 设备的参数，所有 PLC 设备都必须配置 NEK 密钥，这些 NEK 密钥是通过使用配置工具（比如，来自 Intellon 公司针对 HomePlug1.0/Turbo 的 Power Packet Utility，或者是来自 AsokaUSA 公司针对 HomePlug AV 的 Power Manager）来进行安装的。

这种配置工具（可从 http://asokausa.com/downloads/Power Manager1.2-Common.zip 下载）可以在不同的 PLC 设备上配置 NEK 参数。为此，只需要简单地将 PLC 设备一个接一个地连接到通过网线已经安装了配置工具的 PC 上就可以了（根据 PLC 设备模式选择以太网线或 USB 线）。

设备连接到 PC 之后，单击“开始”菜单运行配置工具，如图 10.11 所示，操

作界面将会打开，当前本机连接的网卡将显示在“设备”栏中。“新网络密码”框可用来修改 HomePlug 设定的原始网络密码，还可以为家用网络设定新密码。

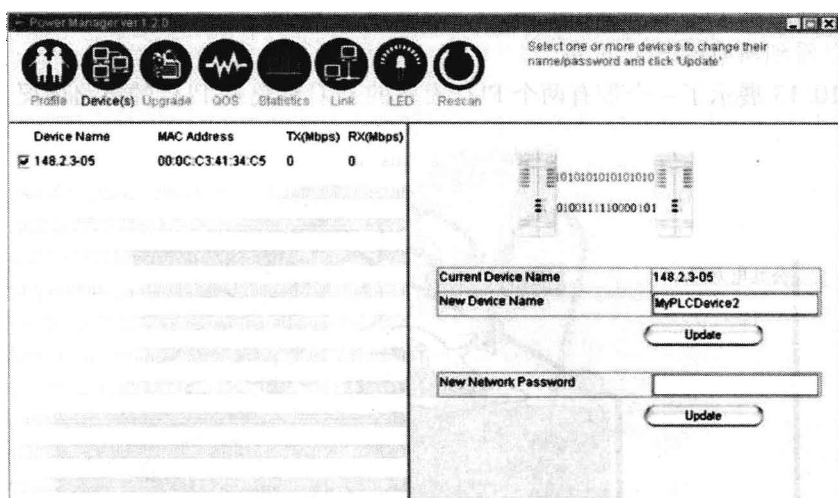


图 10.11　AsokaUSA PLC 配置工具的“产品”页

密码必须是 4～24 位字符，可以包括数字和字母（区分大小写），比如，PLC-Networks。单击针对本机设备安装的“更新（Update）”按钮，如图 10.12 所示，将会弹出“网络加密更改成功（Networks Encryption is Successfully Changed）”的界面，这表明设置已经得到确认。

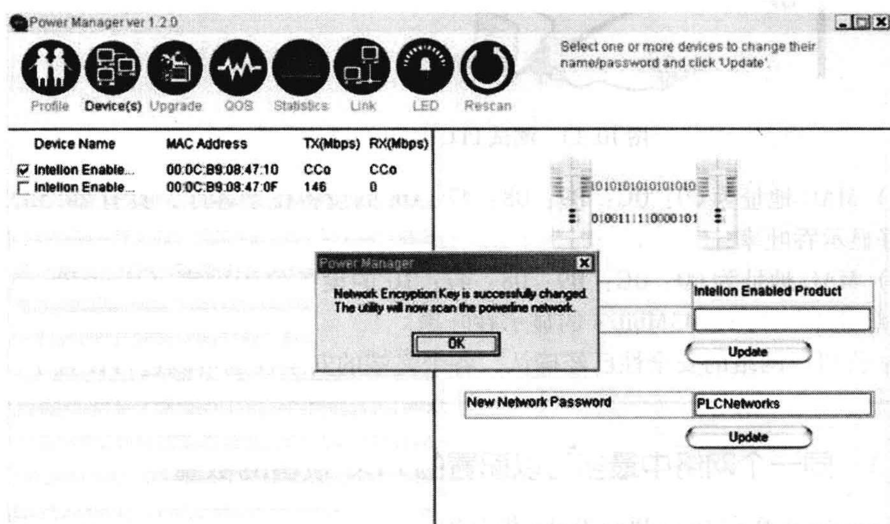


图 10.12　“安全（Security）”页中的 NEK 配置

将各个 PLC 设备连接到配置 PC 上，用同样的方法，就可完成所有 PLC 设备的密码更改工作。

一旦所有的 PLC 设备都正确配置，“设备 （Device)” 栏就能够保证在 PLC 网关上可以看到所有的 PLC 设备。

图 10.13 展示了一个带有两个 PLC 设备的 PLC 网络和 PLC 的链路情况。

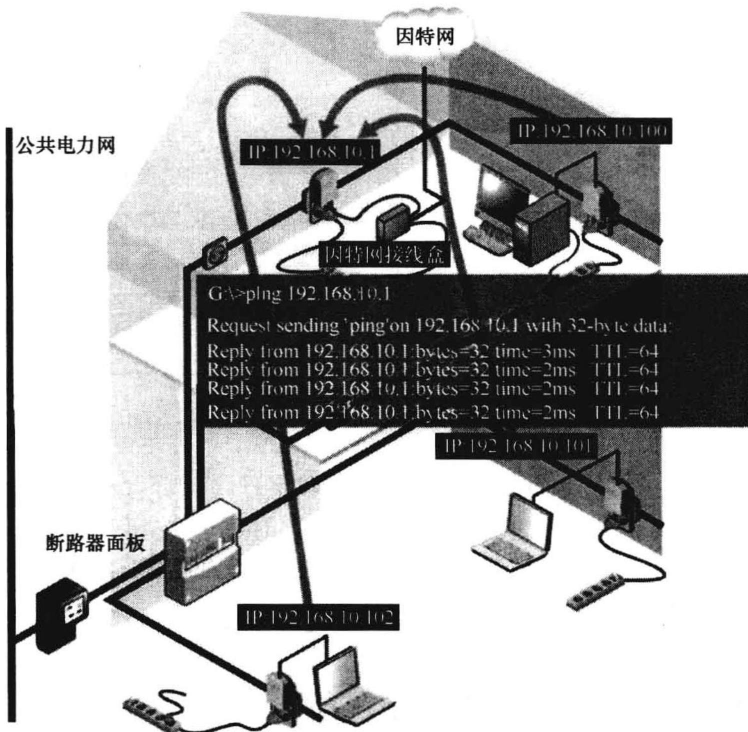


图 10.13 测试 PLC 网络 IP 层示意图

1） MAC 地址为 00：0C：B9：08：47：0F 的设备位于客厅，具有 24.55Mbit/s 的良好显示吞吐率；

2） MAC 地址为 00：0C：B9：08：47：10 的设备位于卧室 （HomePlug 1.0），“第一级速率” 为 13.43Mbit/s 的显示吞吐率。

由于 PLC 网络的安全性已经确认，各个终端的安全性也可以进行设置了。

10.5.3 同一个网络中最多可以配置的 PLC 设备的数量

HomePlug1.0 和 HomePlug Turbo 规范指出，具有相同密码的一个 PLC 网络最多可以有 15 个 PLC 设备。由于不能在 HomePlug1.0 和 HomePlug Turbo 设备上配置多个

NEK 密钥，因此在同一时间，一个 PLC 设备只能属于一个 PLC 网络。HomePlug AV 标准解决了这个问题，该标准可以将不同网络和不同的网络密码配置到一个设备中。

10.5.4 PLC 网络运行测试

网络中各种 PLC 设备设置好之后，建议您可以用 PLC 配置工具（位于“产品”栏中）测试一下已安装好的家用网络的运作是否良好。

为了测试 PLC 网络运作是否良好，我们也可以如图 10.13 所示的那样，在 PC 上运行 ping 命令来测试 PLC 设备与因特网接线盒之间的链路。

为此，所有的 PC 或者终端必须和因特网接线盒的 IP 地址位于同一个地址域内（比如，对于 192.168.10.x 域，因特网接线盒的 IP 地址为 192.168.10.1，其他设备的 IP 地址为 192.168.10.100 或者是 192.168.10.101，192.168.10.102 等)。网络中各设备的 IP 地址配置方法在第 9 章中已详细叙述。

按以下步骤，可以运行 ping 命令：

1）单击“开始”→“运行”；

2）输入“cmd”，打开 Window 虚拟 DOS 界面；

3）输入以下命令：

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply of 192.168.10.1 : bytes =32 time =3 ms TTL =64
Reply of 192.168.10.1 : bytes =32 time =2 ms TTL =64
Reply of 192.168.10.1 : bytes =32 time =2 ms TTL =64
Reply of 192.168.10.1 : bytes =32 time =2 ms TTL =64
```

如果这个命令执行之后立刻就有以上回应显示，就意味着网络配置正确，可以使用了。

10.5.5 防火墙

PLC 与因特网进行连接，就给不怀好意之人以接入家用网络的可能。只有防火墙才能防止这类黑客的攻击。防火墙的作用是，依据连接端口号，仅允许网络内经授权的人使用网络。

每一种协议使用一个特定的端口号（如 HTTP 用 80 端口，可用于被网络识别)。如果仅为应用程序（如电子邮件、HTTP、FTP）开放相应端口，就可以阻止其他端口的使用。

市面上有很多防火墙软件，有一些是免费的，比如使用 2.4 或 2.6 内核的可在 Linux 配电网络中运行的某些防火墙。

Windows XP 操作系统允许为网络工作站建立软件防火墙规则，但不能给一个具

体的物理网络建立防火墙规则。不像硬件防火墙，可以禁止整个网络的某一种协议。

按以下步骤，可以访问 Windows XP 的软件防火墙：

在控制面板，选择“网络连接”，如图 10.14 所示；选择“以太网连接（Ethernet Network Connection）”，打开对话框，如图 10.15 所示；单击“高级（Advanced）”页，再单击“设置（Settings）”按钮，打开 Windows 防火墙对话框，如图 10.16 所示；在“常规（General）”页，选中“启用（推荐）”。

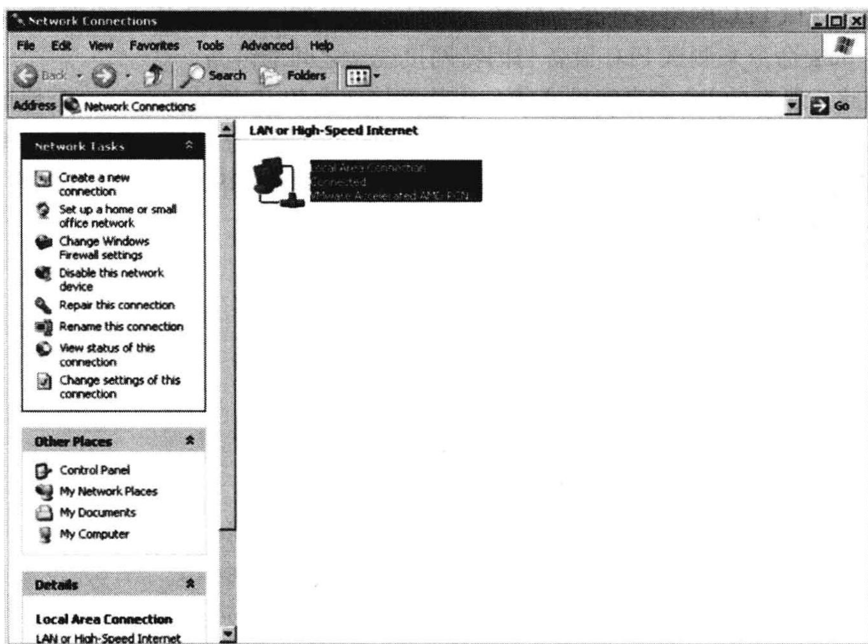


图 10.14 Windows XP 操作系统网络连接窗口

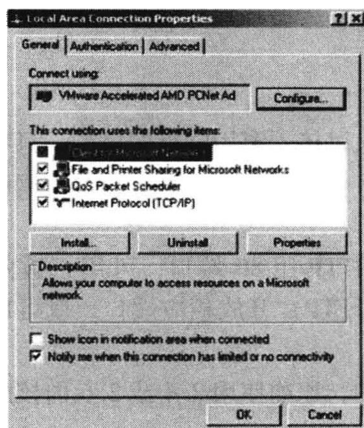


图 10.15 以太网属性对话框

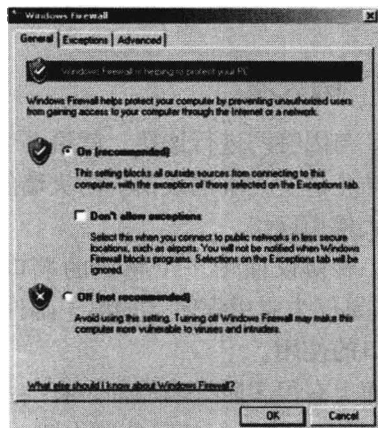


图 10.16 高级防火墙连接配置参数

硬件防火墙必须安装在与因特网直接相连的电脑上。例如前文提及的接入网关，就可以看成是这种理想的专用电脑（见图 10.17）。

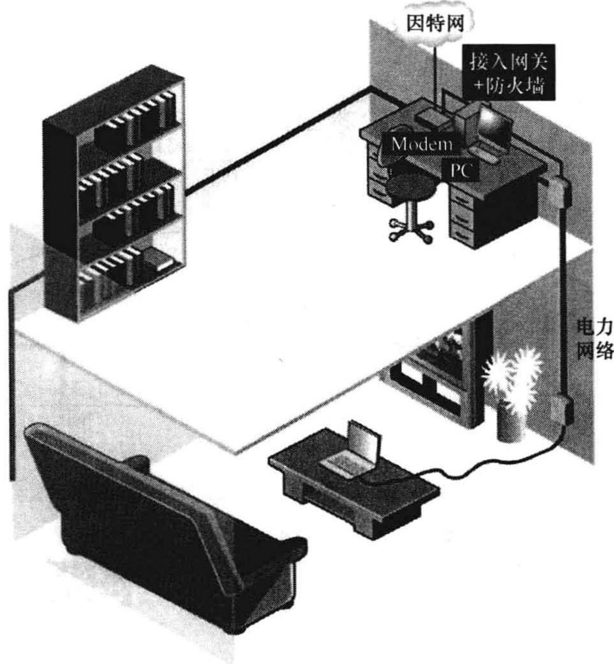


图 10.17 防火墙保护的网关的 PLC 网络示意图

10.5.6 VPN 和 PPPoE

保证整个 PLC 网络安全运行的唯一方法就是第 4 章中所描述的 VPN（虚拟专用网）。

如果网络需要高级别的保护，使用鉴权服务器就显得有必要了。使用鉴权这种方法，顾名思义，就是为了可靠地鉴别每一个想连入网络的用户——RADIUS（远程拨号用户鉴权服务，其中有一种免费的版本叫“Freeradius”，可以在以下网址下载：http://www.freeradius.org，它是应用最广泛的鉴权协议）。

为了在一种更高更可靠的水平上保护网络，VPN 必不可少。VPN 可以通过鉴权和加密机制全面保护 PLC 网络。目前，IPsec 是应用最广泛的 VPN 协议。然而，IPsec 的 VPN 协议需要在高性能的电脑上才能使用，而且该协议还要求客户端电脑拥有 VPN 客户端需要的配置。

若接入因特网的网关，如图 10.18 所示的那样，已经涵盖了 DHCP 和 NAT 路

由器功能，那么使用鉴权服务器或者 VPN 服务器就需要添加相应的功能，以适应特定网关级别。

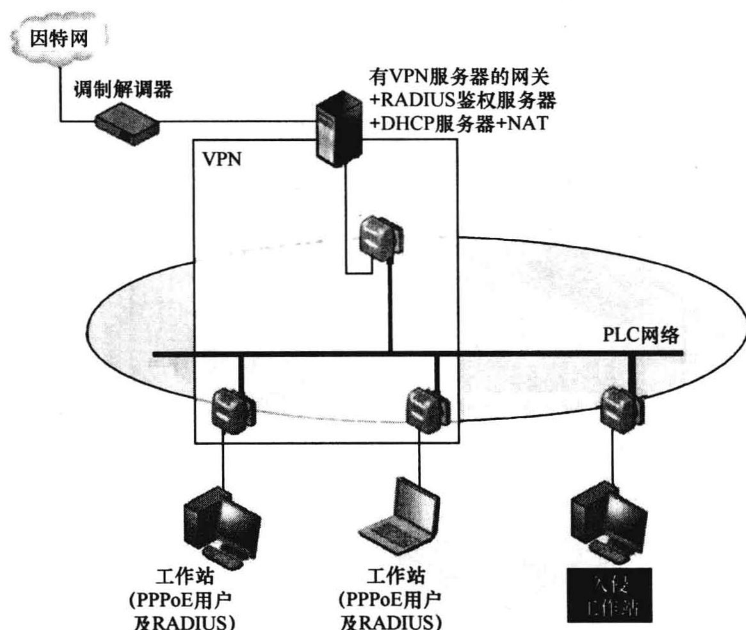


图 10.18 VPN 或 RADIUS 保护的网关的 PLC 网络

另一种提高 PLC 网络安全性和本地 IP 网络安全性的方式是安装 PPPoE 服务器和一个相应的 RADIUS 服务器。这项技术可以为连接到本地 PLC 网络上的计算机和连接到因特网网关的计算机之间提供数据"通道"；这些客户端通过 RADIUS 服务器进行鉴权。

如果一个入侵者成功连接到本地 PLC 网络，只要他没有连接到网关上的 PPPoE 服务器和 RADIUS 服务器，他就不能使用网络。因此，黑客的机器既不能进入连接到 PLC 网络上的其他计算机，也不能通过 PLC 网关访问因特网。

图 10.19 展示出的是，建立在客户端电脑和因特网网关之间的 PPPoE 数据通道的概念，它可以保证网关（与因特网）与客户端电脑之间数据交换的安全。

这项基于 PPPoE 通道的保护技术被因特网接入商（IAP）广泛采用，以确保区分各种网络客户端。它也可应用到 PLC 家庭网络或者专业网络。

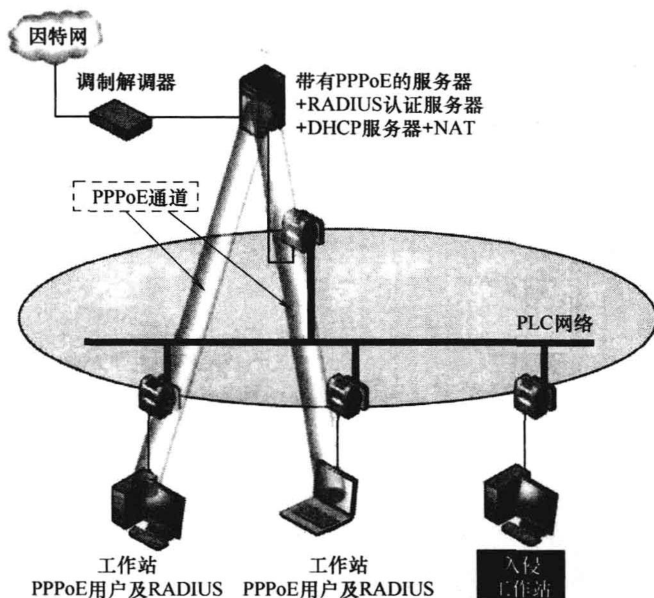


图 10.19　PPPoE 或 RADIUS 保护的网关的 PLC 网络

10.6　配置因特网网关

在 PLC 网络中，可能会有各种网络连接方式：56K 调制解调器、ISDN、同轴线缆、ADSL、ADSL2 +、卫星或者 FTTH（光纤到户）。因为 PLC 网络的传输速度对于 HomePlug1.0 来说，是 1 ~ 14Mbit/s；对于 HomePlug Turbo 来说，是 1 ~ 85Mbit/s；对于 HomePlug AV 来说，是 1 ~ 200Mbit/s，这大致满足了当前所有可用因特网接入方式的吞吐率。

HomePlug1.0 的性能可以产生低于最新 ADSL 技术（如 ADSL2 +）的 20Mbit/s 的数据吞吐率，不过当您使用 HomePlug Turbo 时，就能有 25Mbit/s 的传输速率，传输速率问题迎刃而解。

可以按以下两种不同的方式进行因特网共享连接：

1）通过专用计算机，或者将 PLC 设备直接连接到用于访问因特网（因特网接线盒）的调制解调器；

2）直接使用 PLC 带有调制解调功能的路由器。

在第一种方式中，如图 10.20 所示，一台电脑共享了它的网络连接。

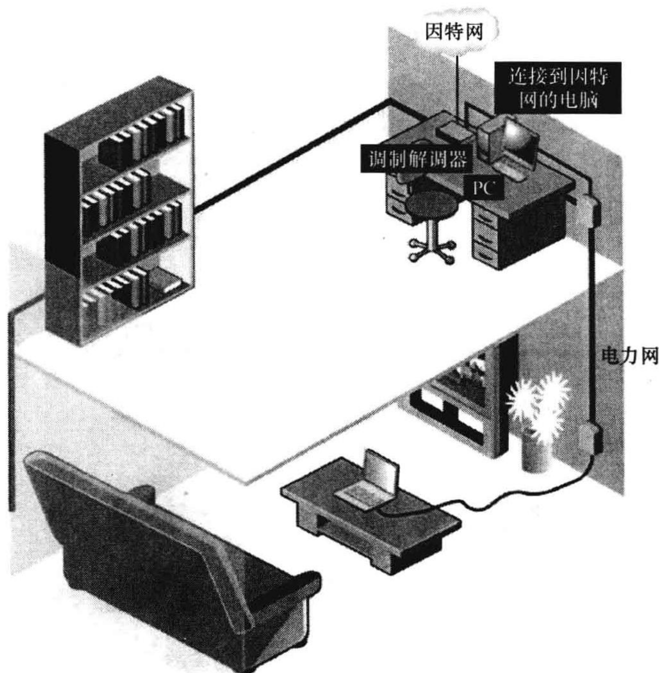


图 10.20 通过专用计算机共享上网示意图

图 10.21 展示的是一个通过多功能（xDSL/PLC 调制解调器/路由器）设备连入因特网的家用 PLC 网络。

这种网络类型的不足在于，PLC 设备仅使用一个防火墙来阻挡各种数据流、避免对网络或者 VPN 的攻击。在这种使用专用电脑来进行因特网连接的网络拓扑中，可以安装各类软件防火墙和 VPN 服务器软件，以保护网络。

10.6.1 网络共享连接

为了实现网络共享，可以使用两种协议：NAT（网络地址翻译）和 DHCP（动态主机配置协议）：

1）NAT 使用 ISP 提供的 IP 地址，可以为多台工作电脑提供因特网共享服务。NAT 的另一个独特的功能就是，这种共享可以保护您免受一些攻击。一些带路由器功能的因特网调制解调器内嵌了 NAT 协议，不过 NAT 也可安装在接入网络的专用电脑上。

2）DHCP 是一种客户端—服务器协议，可以动态地分配 IP 地址，这需要花一些时间，因为客户端电脑需要配置 TCP/IP 参数，以连接到网络。这些由 DH-CP 服务器提供给客户端的参数有 IP 地址、子网掩码、默认网关和 DNS 服务器地址。DHCP 提供便捷的用户配置界面，这些配置也可以通过直接修改广播参数来手动操作。

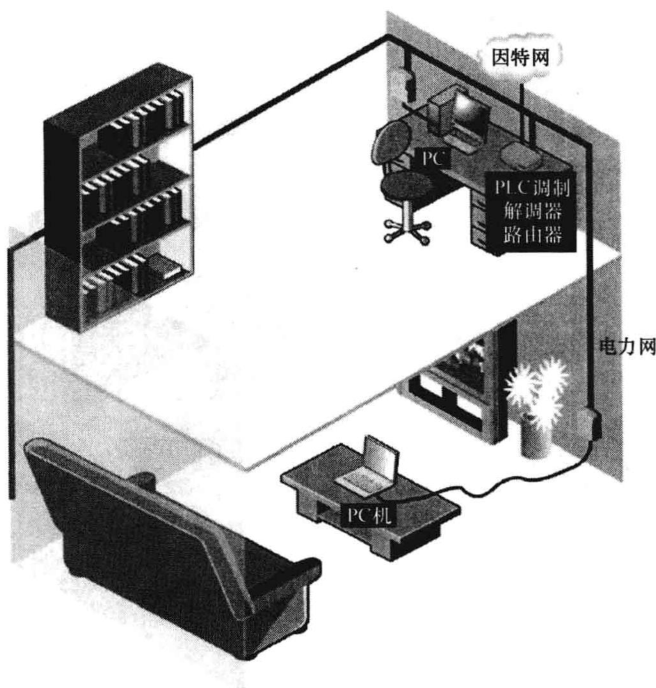


图 10.21　由 PLC 路由器实现因特网连接示意图

DNS 地址

DNS 地址由 IAP 提供，除非局域网有自己的 DNS。

只要涉及 IP 地址，如图 10.22 所示，所有的网站都必须有同样的网络地址段，例如，192.168.0.x 或者 10.0.x.x，这里，x 是介于 1 ~254 之间的整数。

10.6.2　设置 NAT 和 DHC

PLC 家庭网络的理想结构是，PLC 路由器既能用作 NAT 路由器又能用作 DHCP

服务器功能的结构，其中 NAT 可以将局域网中的所有设备进行网络连接的共享，DHCP 则为每一个设备提供接入网络的参数。现在家庭 PLC 设备市场上的带路由器功能的调制解调器都渐渐包含了这些功能。

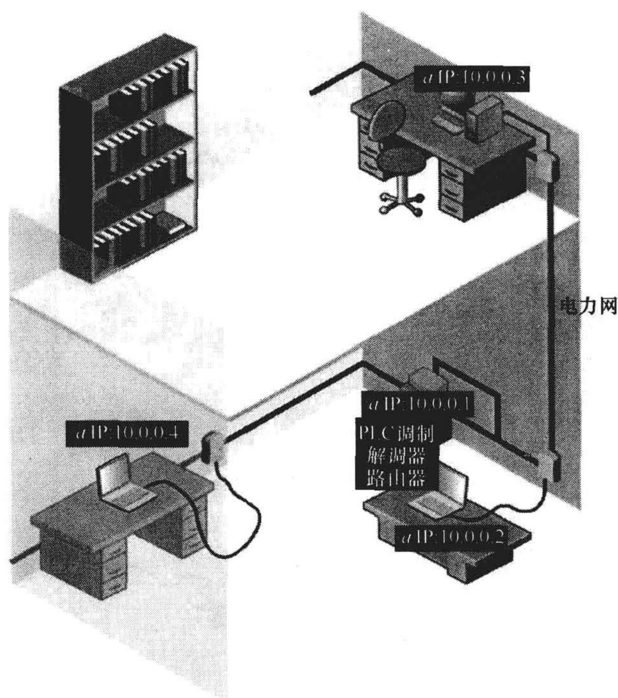


图 10.22 配置家庭网络的 IP 地址

这种理想的家庭网络结构如图 10.23 所示。

在 NAT 和 DHCP 功能没有嵌入因特网调制解调器或作为网关的因特网接线盒的情况下，仍然可以使用这两种协议，只是需要如图 10.24 所示的那样，配备一台作为网关的专用电脑。

为了配置这种专用电脑，最好使用 Linux 操作系统，因为各种版本的 Linux 操作系统都提供 NAT 和 DHCP 功能，而 Windows 操作系统必须使用收费软件。Linux 操作系统的另外一个优点是，它不需要巨大的资源。

为配置一台使用 NAT 并且包含了 DHCP 的电脑，仅占用 48% 的处理器资源和 32MB 的存储器就绰绰有余了，这种电脑的另一个优点是，它可以保持 24h 无障碍运行。

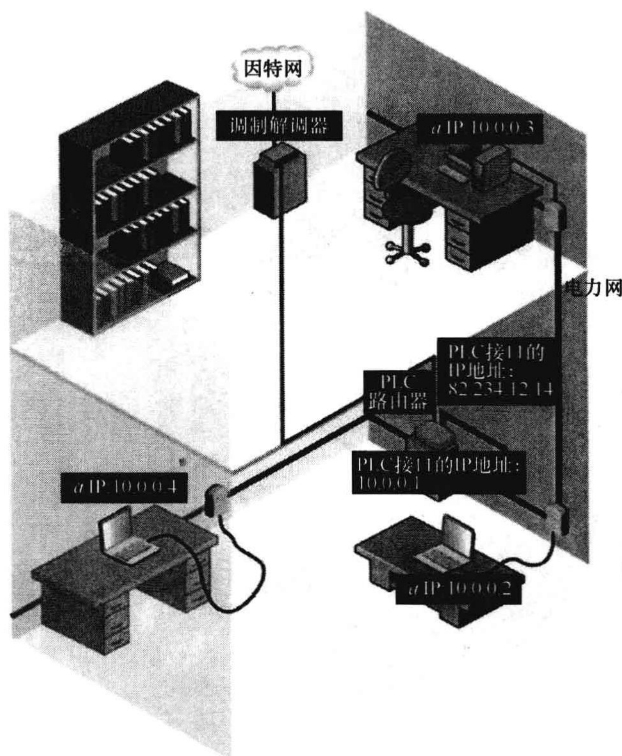


图10.23　理想的PLC家庭网络结构

DHCP（动态主机配置协议）

DHCP可以给局域网中的站点动态地提供IP参数。该协议让管理工作变得更加简单，当需要管理大量电脑时尤为明显，因此DHCP得到了越来越广泛的应用。

DHCP原本是想设计成为另一个具有相同特点的协议，即BOOTP。BOOTP的信息与DHCP兼容，不过反之则不然。DHCP和BOOTP的不同之处在于：DHCP可以向各站点提供指定范围内的IP地址，这些地址都是经过协商的，并且只在指定的一段时间内有效。

DHCP结构

DHCP是基于客户端—服务器结构的。在PLC网络中，DHCP客户端就是PLC网络中的设备，DHCP服务器就是带调制解调功能的PLC路由器。

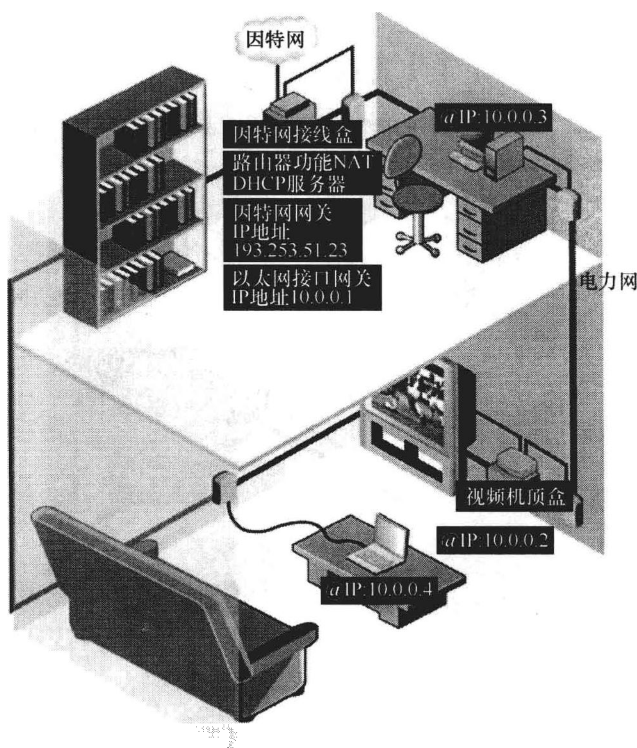


图 10.24 通过专用网关联网的 PLC 家庭网络结构

在图 10.25 所示的例子中，只有一个 DHCP 服务器，它处于 IAP 提供的因特网接线盒层级或者是因特网调制解调器层级。由于网络中用于接入因特网的网关有数个，因此就可以有多个 DHCP 服务器。使用多个 DHCP 服务器并不会引起网络冲突。

当一台电脑初始化时，DHCP 就向它提供以下参数：

1） IP 地址；

2） 子网掩码；

3） 默认网关；

4） DNS 地址；

5） 域名。

收到这些参数之后，这台计算机就可以自由地与网络中的其他计算机对话，如果其他计算机共享了因特网连接，那么这台计算机也可以由此接入因特网。这是一种耗时不超过 1s 的用户透明机制。

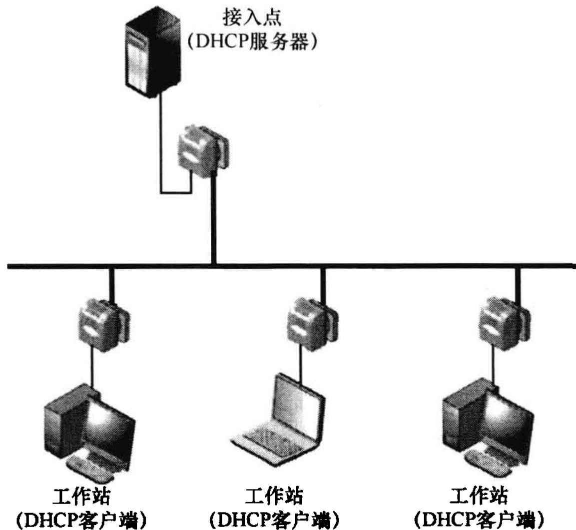


图 10.25　DHCP 结构

DHCP 的另一个特殊功能就是租用。如前所述，提供给网站的参数只在一段给定时间内有效。这种租用期是在需要参数时，由计算机和服务器协商制定的，当租用期过期后，计算机还可以重新协商生成。

DHCP 客户端动态配置

一台计算机连接到 DHCP 服务器的动态配置有 4 个过程，如图 10.26 所示。

1）当 DHCP 客户端接入网络，没有地址分配，其地址为 0.0.0.0。

2）为了配置其 IP 地址，客户端以广播模式在网络中发送 DHCP DISCOVER 请求，地址为 255.255.255.255，同时加入其 MAC 地址。

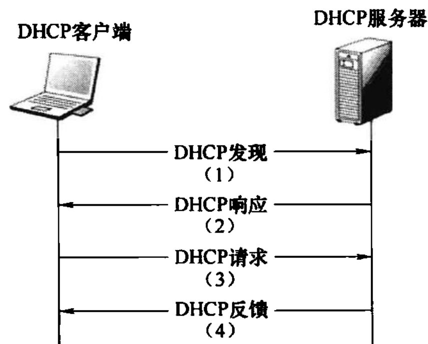


图 10.26　DHCP 动态配置一台计算机的过程

MAC 地址

MAC 地址是分配给 PLC 网络中每一个以太网卡终端的固定地址。

● 因为客户端此时还没有 IP 地址，DHCP 服务器就按照广播模式反馈 DHCP OFFER，DHCP OFFER 消息由客户端 MAC 地址、租用时间和一些 IP 地址组成。

现实中可能有多个 DHCP 服务器，但我们在本书中只考虑一个 DHCP 服务器的情形。

3）如果客户端接收到了这个 OFFER 消息，就发出 DHCPREQUEST 消息，以接收后续参数。

4）服务器发送 DHCP PACK，以确认客户端被正式接受。

在 Windows XP 中的配置

在 Windows XP 下配置 DHCP 客户端，非常简单。

1）在 Windows 环境下插入一块以太网卡，系统会自动配置其为 DHCP 客户端；

2）如果网卡已经被设定了一个固定 IP，打开控制面板，选择“网络连接（Network Connection）”，如图 10.27 所示；

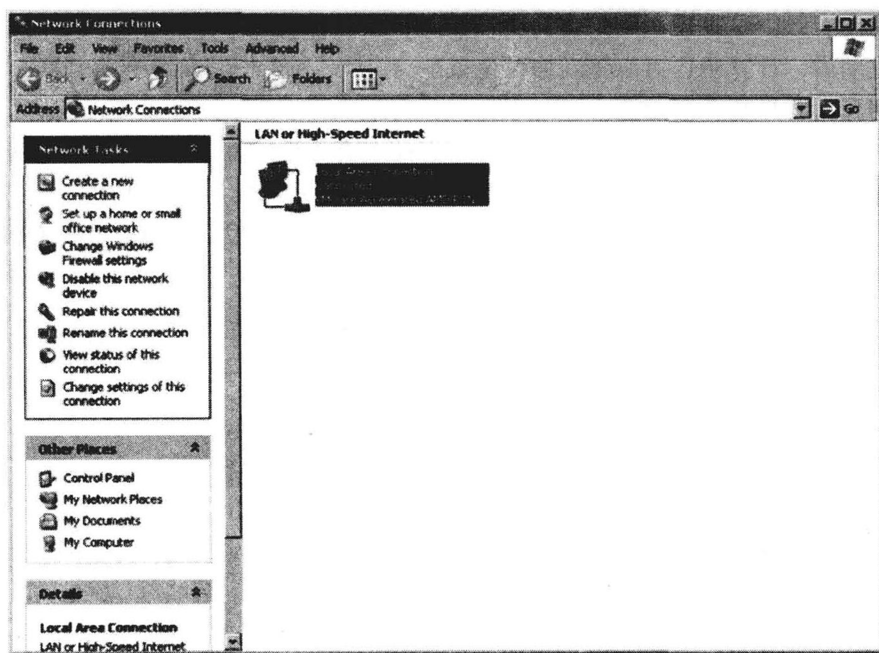


图 10.27 网络配置（这里 PC 中还有一个 Wi-Fi 连接）

3）选择“连接到局域网”，如图 10.28 所示；

4）单击“属性”，弹出局域网的属性框，如图 10.29 所示；

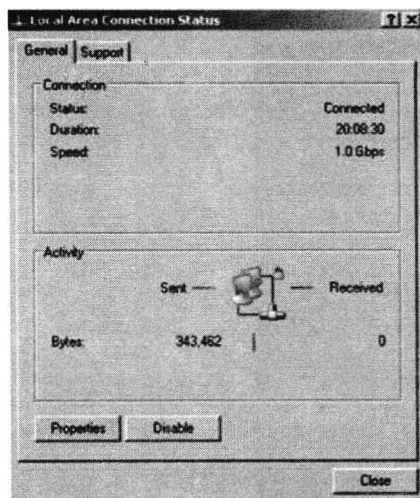


图 10.28　连接到局域网络的情况

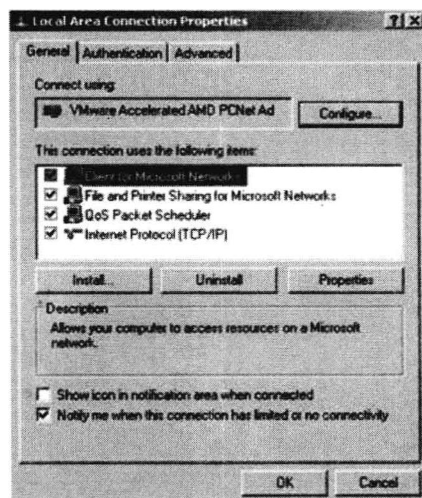


图 10.29　局域网络连接的属性

5）双击选中“Internet 协议（TCP/IP）”框，弹出“Internet 协议（TCP/IP）属性（Prosperities of the Internet Protocol（TCP/IP））”对话框，如图 10.30 所示；

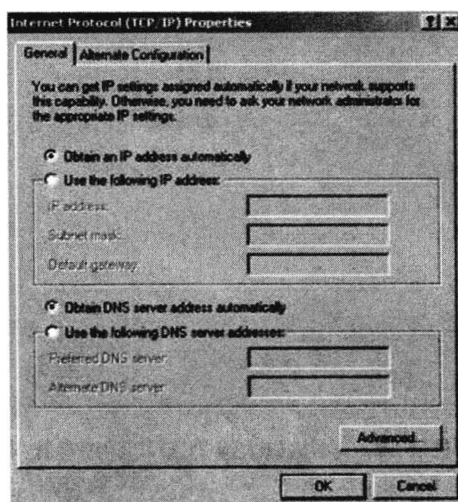


图 10.30　配置局域网卡的 TCP/IP 参数

6）选中“自动获得 IP 地址”，电脑就完成了 DHCP 配置。

在 Windows 2000/XP 操作系统下，要想检查网卡是否已经配置好，只需确认其处于“局域网连接状态”就可以了，如图 10.31 所示。

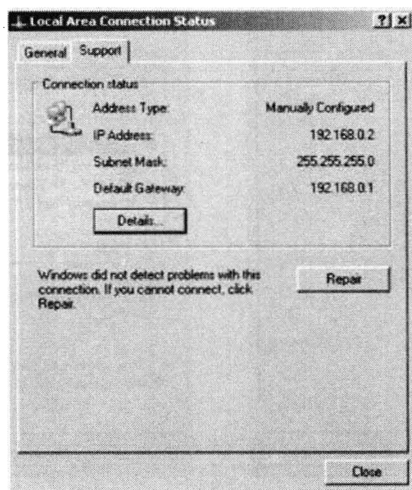


图 10.31　本机 TCP/IP 参数

“详细信息（Details）”按钮能提供有关网卡参数的更多信息（见图 10.32）。

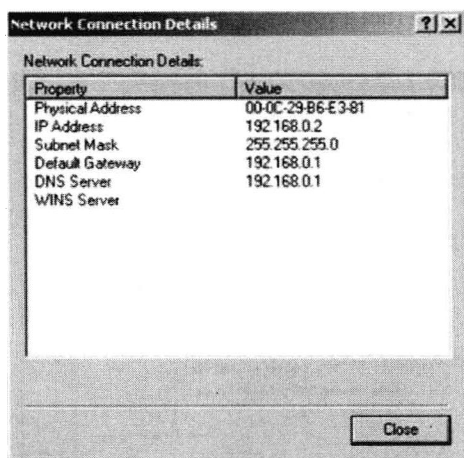


图 10.32　本机以太网 TCP/IP 详细参数

也可以通过 ipconfig 命令检查网卡配置：

1）在开始菜单，单击“运行”，输入 cmd 命令，打开 MS-DOS 界面；

2）在提示符后面输入 ipconfig/all，当前网卡的所有信息就显示出来，此时可

以检查其是否配置好了。如图 10.33 所示，我们可以看到其列出了与我们前面所述一样的信息。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\OP>ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : as_winxp_workst
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter

        Physical Address. . . . . . . . . : 00-0C-29-B6-13-81
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\OP>_
```

图 10.33　ipconfig 命令显示的 TCP/IP 参数

如果网卡没有被 DHCP 服务器配置好，那么 Windows 系统会自动分配一个默认地址 169.254.x.x 给网卡。为了向 DHCP 服务器发出重新初始化的申请，可以输入 ipconfig/release，然后输入 ipconfig/renew。

第 11 章　PLC 在商业中的应用

PLC 网络越来越多地涌入商业领域、专业网络和工业领域中，PLC 网络甚至替代了 Wi-Fi 以及以太网络。

正是因为 PLC 网络的性能以及在电网中能够长距离传输的特点，PLC 网络不仅可以作为中小企业的骨干网，还可以作为专业（酒店、医院、礼堂、超市等）和企业（工厂、仓库、起吊系统等）建筑物的骨干网。

因此，PLC 网络可以作为取代其他企业网络的技术，也可以成为这些网络的有益补充。在下面的情形中，这一情况更为明显：

1）为节省经费或者建筑物中的设备不能搬移（因机密而受保护的建筑、医院等），PLC 网络可作为骨干网而代替以太网；

2）为了更好地满足人们对扩展当前以太网（因其价廉、易部署等）的需求，PLC 网络可以作为一种补充手段；

3）在某一场活动（音乐会、会议等）中，PLC 网络可以作为临时网络；

4）在同一个电力线网络（管理部门、警察、图书馆等）中，PLC 网络可以组建多个不同的网络。

PLC 设备的价格不是很高，特别是对那些完全使用 PLC 网络的企业而言，由于节省了有线设备的投资（线缆、插座、交换机等），从长期的眼光来看，使用 PLC 网络是相对合理和经济的。

在一家企业中，PLC 网络可以作为一个工作网络，或者是作为一个网络供客户使用，比如，客户可以通过它访问因特网。在后一情形中，使用 PLC 网络便能够既满足客户的需要，同时又将客户与企业网络隔离开来。

第 10 章着重介绍了 PLC 家庭网络安装等有关内容，本章将叙述 PLC 用于企业网络的安装和配置，尤其是在接入电力网时的安装和配置。

11.1　网络结构

在一家企业中，根据网络规模的大小、拥有网站的数量和网络承担任务的不同，各个 PLC 网络结构之间的差异很大。

拥有少量计算机（少于 10 台），并且通过 ADSL 或者有线调制解调器上网的小企业，其网络结构与家庭网络结构没有区别。

在商业网络中，唯一需要考虑的 PLC 网络结构上的问题就是关于 DHCP 服务器、NAT 路由器以及连接到因特网的专用网关的选取问题。此外，也可以在同一个电力网上设立多个 PLC 网络，即采用增添一个或多个 PLC 网关的形式进行交换式连接。

在图 11.1 展示的这个结构中，有一台服务器扮演了 DHCP 服务器和 NAT 路由器的角色，交换机与之相连，可以通过新的 PLC 网关接入这个网络。

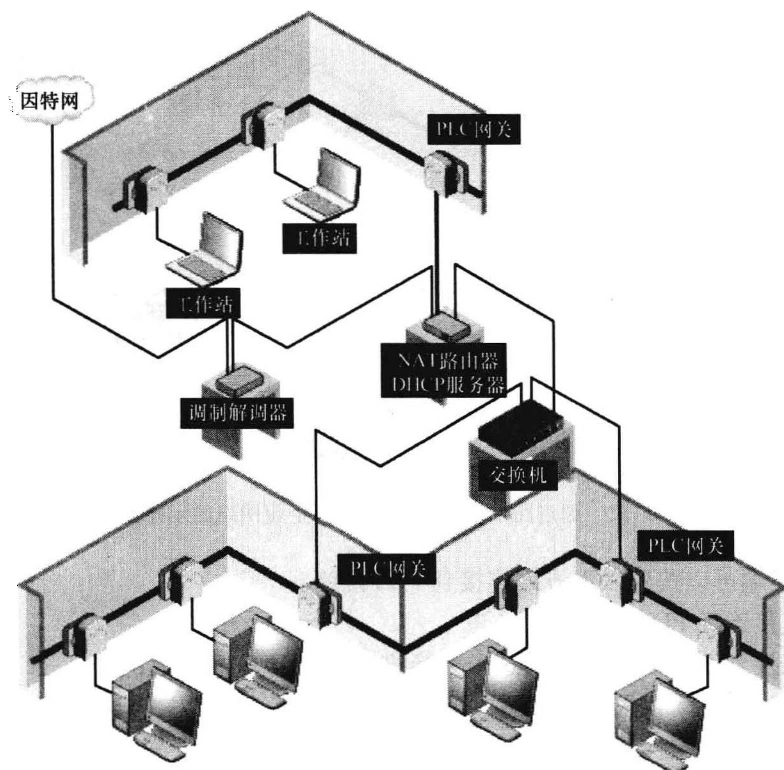


图 11.1 多个 PLC 网关和一个交换机组成的 PLC 网络结构示意图

最常见的情况是，PLC 网络在企业现有的网络基础之上建立，要知道，企业的现有网络已经有了 DHCP、NAT 的功能并且与因特网相连接。

图 11.2 展示了企业中包含的两个子网，这两个子网之间通过两个路由器，建立起广域网（WAN），从而彼此相连。企业每一个区域的以太网都与路由器连通，PLC 网络用于连接企业房间中的各个终端，该网络也连接到以太网上。

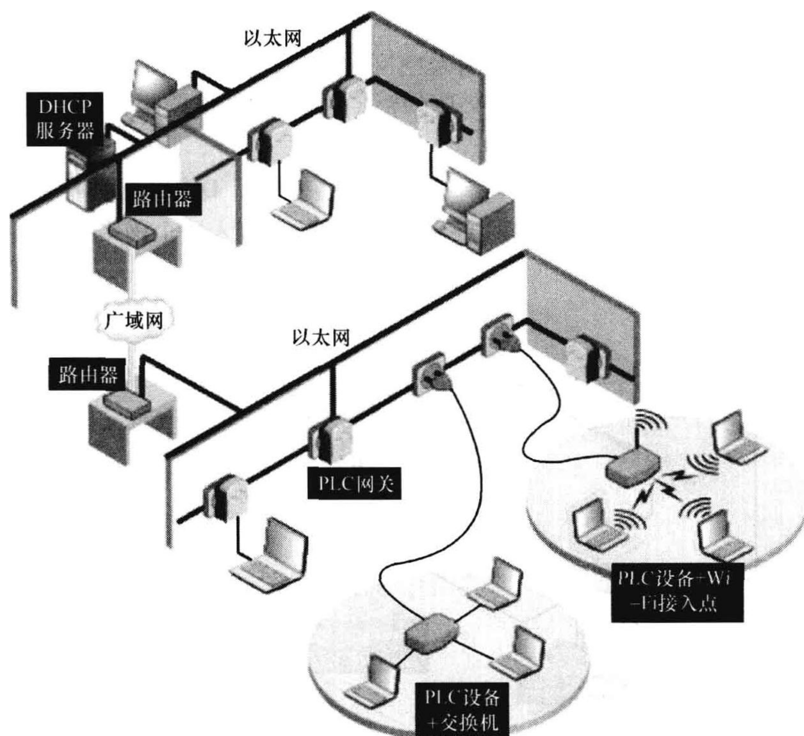


图 11.2 通过路由器将 PLC 网连入企业网络的示意图

用户终端可以按照以下方式连接到 PLC 网络：

1） 直接连到 PLC 设备上；

2） 连接到 PLC 交换机，而这个交换机连接到 PLC 网络上；

3） 通过 Wi-Fi 接入到内置 Wi-Fi 功能的 PLC 接入点上，再连接到 PLC 网络。

监管 PLC 网络

专业网络和工业企业对网络的需求与家庭网络不同（例如在监管上），专业网络和工业企业网络需要具有一些额外功能，从而确保网络能够长期正常运转，并能在某些网络设备出故障时向管理员报警。

在众多用于监管的规范性协议中，简单网络管理协议（SNMP）V1、V2 和 V3 版本在装有了 SNMP 组件的网络设备中应用较多。这种软件可以监视远程的网络设备，获取一些网络和系统的参数（丢包、接收到的包、主板温度、CPU 转速等）。

考虑到 PLC 技术运行在数据链路层（MAC 层），故目前还不能直接用于远程 SNMP 监管。不过很多硬件和软件工具可以用于监管 PLC 网络。

图 11.3 介绍了监管多个 PLC 网络所采用不同的技术。AsokaUSA、DS2 和 Spidcom 直接在各自的设备中设有 HTTP 接口和 SNMP 堆栈。

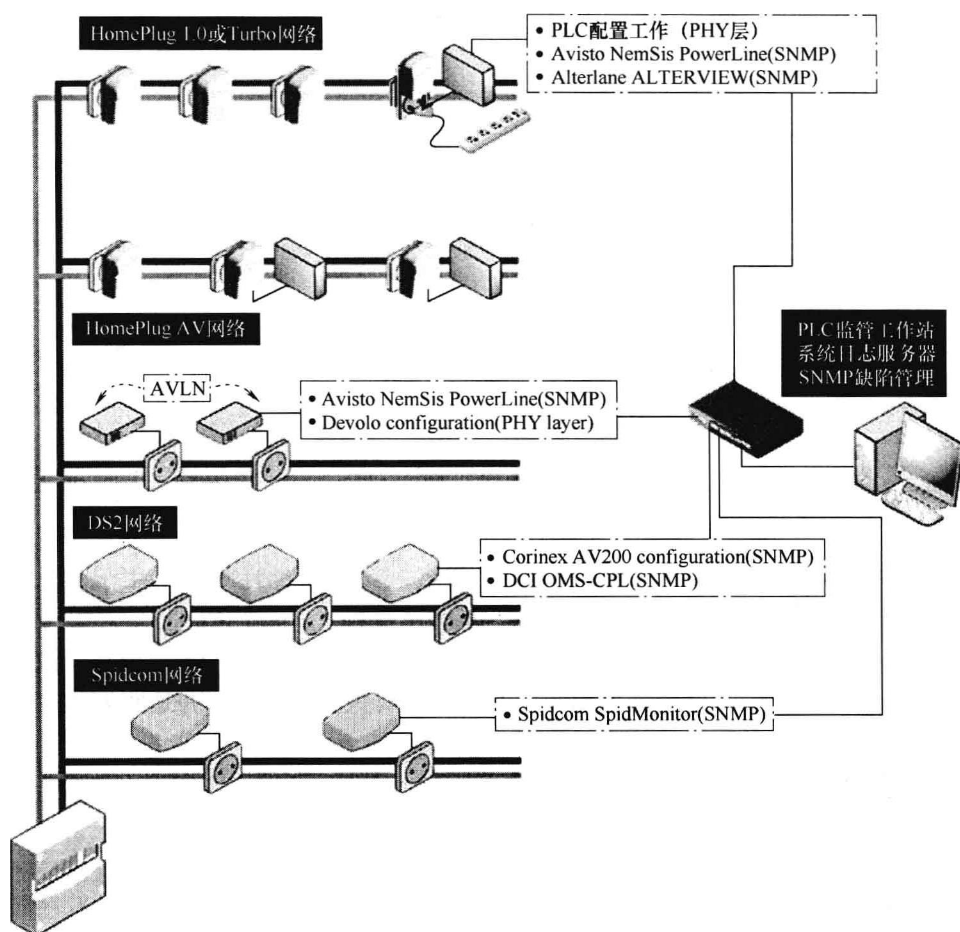


图 11.3　不同 PLC 网络技术的统一监管工具

由于 HomePlug（1.0、Turbo 和 AV）技术在它们的设备中没有包含 SNMP 堆栈，因此有必要在 MAC 层开发监管工具，并且使用这些能够监管 PHY 层中 PLC 链路状态的配置工具。

11.2　选择标准

不同于家用 PLC 网络，对专业网络和工业企业网络而言，设备的价格是一个主要因素，并且对功能往往有一定的要求。这就意味着，要选择一种更专业的技术、选择一种尽可能开放的标准，从而将来可方便地进行升级。

表 11.1 列出了企业 PLC 技术的多种选择标准。

表 11.1　几种企业 PLC 网络技术的标准的选择

PLC 技术		选择标准
HomePlug	1.0，Turbo	价廉，适用于 SMB，少量高级功能，DES 56bit，易安装，维护量少
	AV	领先的技术，高速的有效吞吐量，价格昂贵，高级网络管理功能，可靠的 QoS
	AsokaUSA	与 HomePlug 1.0 和 Turbo 兼容，高级功能（HTTP 接口、单 IP 地址 SNMP 管理、加固等），专业电线耦合系统，PLC 中继器
DS AV200		高速稳定的吞吐量，主-从结构，中央式管理，与 HomePlug 1.0 和 Turbo 不兼容，产品可集成到专业包中，高级配置功能（安全、QoS、虚拟网等）
Spidcom		高速稳定的吞吐量，更高级的配置（可能为每个频率子带配置），中央式管理（SNMP、HTTP 等），有在 PLC 领域中创新产品的应用经验

AsokaUSA 公司为专业人士开发了基于 HomePlug 规范的产品。采用这种规范的产品能够兼容 HomePlug 1.0、Turbo 和 AV 设备。该公司也计划推出用于优化 PLC 网络的产品和附件（如中继器、滤波器、耦合系统）。

Devolo 公司也为专业网络开发了 HomePlug（1.0、Turbo 和 AV）产品，该产品安装在一个金属箱中。这个金属箱装配有系统的有关附属设施，并适宜安放在工业企业建筑物电力设备附近的技术操作间之中。

11.3　选择网络和电力设备

家庭 PLC 中选择网络和电力设备的标准在商用 PLC 网络中也适用，不过需要补充一些其他的要求才行，特别是以下几个要求：

1）可管理超过 15 个设备（同一个 PLC 网络中限 HomePlug1.0 和 Turbo 这两种标准）；

2）网络监视功能（如 SNMP）；

3）集中管理和配置功能（如 HTTP、Telnet、SSH 等）；

4）与 PLC 电力设备散热金属盒有隔离；

5）PLC 接口，并且有独立的 110 或 220V/50 或 60Hz 的电力供应；

6）可能的 PLC 信号中继功能；

7）集成高级网络功能（NAT 路由器、DHCP 服务器、防火墙、交换机、Wi-Fi 等）。

只要涉及 PLC 设备（如滤波器、耦合系统、PLC 信号注入器），建议使用专业产品，并在专业电力工程师的帮助下安装，以确保符合安全标准，获得长期稳定的安装。

11.3.1 服务质量

随着视频、HDTV 视频流广播、IP 电话、计算机支持的协同工作、视频会议等实时应用的发展，很需要将服务质量（QoS）整合到不同的 PLC 技术中。

使用 PLC 网络实现这些技术很难解决的一个问题就是网络本身的限制，这是因为 PLC 技术用作通信的媒介，很容易受到连接到网络上的其他设备干扰的电力网络。

表 11.2 总结了各种 PLC 技术应用拥有的功能，这些功能可以解决上述提到的技术难题。

表 11.2 PLC 技术的 QoS 功能

PLC 技术		QoS 功能
HomePlug	1.0 Turbo	与 IEEE 802.1Q 规范中的 VLAN 标签相对应的 CA 优先级（数据帧内部的 PRS ）
	AV	与 IEEE 802.1D 规范中业务等级对应的用户优先等级（0～7），Sychro AC，TDMA，QMP 传播，IEEE 802.1Q 规范中的 VLAN 标签的使用
	AsokaUSA	PLC 优先级（VLAN，固定，公平的），优先等级（0～5），受限于信源（IP 或 MAC），受限于信宿（IP 或 MAC）（上行链路和下行链路吞吐量）
DS2 AV200		默认优先级，规范化参数，偏移的使用，模型，掩码，IEEE 802.1Q 规范中 VLAN 标签的使用
Spidcom		适用于在关键应用中对时间 QoS 要求高的 IEEE802.1Q（VLAN 标签）和 IEEE802.1P 规范

这些技术中，HomePlug 1.0 和 Turbo 也许只能提供最少的 QoS 保障，而对于 HomePlug AV 而言，只要 PLC 信号以 110 或 220V/50 或 60Hz 的形式在电力网络上传输，并且与 PLC 网络上的其他设备同步就可以提供更优化的 QoS 保障。

HomePlug AV 的 QoS

与 Homeplug1.0 和 Trubo 相比，HomePlug AV 规范得益于 HomePlug1.0 和 Turbo 的发展，并得益于它与这两种 PLC 技术在功能上兼容。在这三者中，通过带有稳定性能的业务流量分级的形式实现 QoS 的应用。AV 名字本身包含了语音和视频这两种应用，在这两种应用类型中，为了防止数据丢失，保证良好的传输质量，QoS 要求（例如理想的高吞吐率、传输时间、抖动）就显得尤为重要了。

如果实现以下功能，那么前述的那些局限性是可容忍的（可参见第 3 章）：

1）PLC 信号于 50 或 60Hz 同步，以保证 TDMA 和 CSMA/CA 与 CP（竞争时隙）和 CFP（非竞争时隙）在时间上的配合；

2）CM（竞争管理）、CCo（中央协调站）和 STA（工作站）设备中 QMP（QoS 和 MAC 参数）；

3）在不同的网络设备之间能够传送QMP，从而保证PLC网络具有均一的QoS以及性能。

在众多QMP参数中，表11.3总结了QoS管理的最重要的参数。顺便提一下，MSDU（MAC服务数据单元）是数据链路层的MAC层中的数据帧。

表11.3 HomePlug AV的主要QoS的QMP参数

QMP参数	描 述
Delay bound（延迟限度）	在发送端数据链路层convergence子层将MSDU帧发送至SAP（业务接入点）的起始时刻和在接收端SAP层接收到MSDU帧的时刻，这两个时刻之间的最大时间值，以ms计算
Jitter bound（抖动限度）	在SAP层的发送端和接收端之间传播一个MSDU数据所需的时间偏差最大值，以ms计算
标称MSDU	基于IEEE 802.3规范的MSDU帧中数据部分的标称值（介于46~1500B之间）
最大MSDU	MSDU帧的数据部分的最大值
最小MSDU	MSDU帧的数据部分的最小值
Average data rate（平均数据传输速率）	通过PLC链路在SAP的convergence子层传输MSDU帧的平均传输速率，以10kbit/s为单位计算。这并不包括传送MSDU帧所需的MAC和PHY层帧头
最大数据传输速率	通过PLC链路在SAP的convergence子层传输MSDU帧的最大传输速率
最小数据传输速率	通过PLC链路在SAP的convergence子层传输MSDU帧的最小传输速率
Max burst size（最大突发长度）	由应用程序以最大传输速率产生连续的MSDU帧，直至溢出时的最大长度，以B为单位表示
MSDU error rate（MSDU错误率）	MSDU的错误率，以$x \cdot 10^{-y}$表示，其中x指的是无符号整数格式中8位最重要的位，y指的是相同格式中8位最不重要的位
Inactivity interval（闲置时间间隔）	在CM（连接管理）设备决定重传之前，无数据传输，连接能保持空闲状态的最长时间，以ms计算
CLST	业务接入点的convergence子层与IEEE802.3标准中相应子层的兼容性
CDSEC（连接描述）	上层应用或HLE（高层实体）的可选项，可用于UPnP（通用即插即用）模式的QoS，或其他应用层。这些数据域是IP版本（v4或v6），源IP，目的IP，源IP端口，目的IP端口，IP（UDP或TCP）
ATS容限	可容忍的误差，以μs计算，PLC网络同步时钟或者NTS（网络时钟基础）与MSDU帧的ATS时间戳之间的偏差
每个TXOP的平均PB数	PLC链路中，传输两次MSDU帧之间的520B PHY层的平均数据块数量
每个TXOP的最小PB数	PLC链路中，传输一个MSDU帧所需的最小物理层520B数据块数量
每个TXOP的最大PB数	PLC链路中，传输一个MSDU帧所需的最大物理层520B数据块数量

我们可以看到，HomePlug AV 的 QoS 管理是很复杂的，它需要使用很多参数，按照设定要求在网络设备之间进行交换。

这样的 QoS 管理解决了这些应用面临的网络局限性的问题。如表 11.4 所示，对应于用户不同的优先级，HomePlug AV 规范了 8 类应用。

表 11.4　用户可定义的应用优先级

用户等级	应用分类
7	网络检查（特点是保证接收数据包，以管理网络基础设施）
6	语音（传输时延小于 10ms，已知的最大值可能出现在校园局域网的交叉点）
5	视频和音频（传输时延小于 100ms）
4	经验证的网络业务（典型用于准入验证的专业应用和为保证某些传输时间而预留的带宽）
3	白金（通常为“尽最大努力”的 PLC 网络的一些特权用户类型的使用）
1，2	背景业务（通常用于文件传输和其他重要的业务，对余下的 PLC 网络应用无影响）
0	最大努力（通常为常用的 LAN 业务：电子邮件、Web 浏览器、FTP、IRC 等）

11.3.2　接入电力媒介

如第 7 章和第 10 章所述，主要有以下两种方法接入电力媒介：

1）容性耦合，就像使用一件家用电器一样，将 PLC 设备如网关、网络设备（见图 11.4）插进插座。

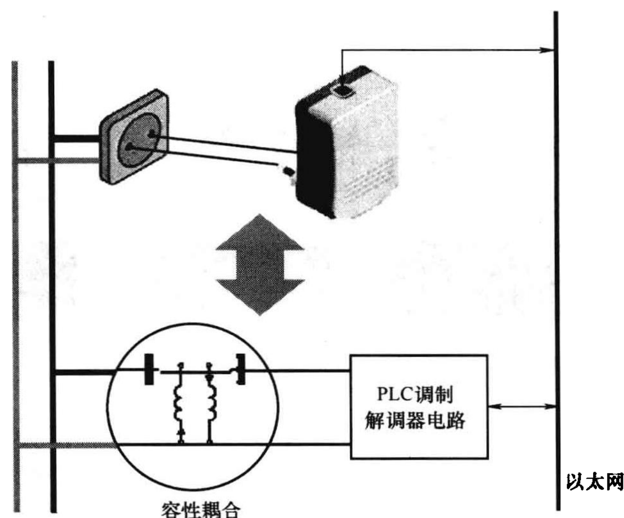


图 11.4　PLC 设备通过电容与电力网耦合原理图

2）感性耦合，比线缆更有效地传送 PLC 广播信号，且性能更好。然而，这一耦合方式需要接入到电力线上。在操作上，只能在断路器控制面板处，针对每一根电缆（或者同时针对几根电缆）采用耦合或者注入的方式实现。

图 11.5 示出了在断路器控制面板处的三相电力线上，PLC 信号的各种接入方式的原理示意图。当然了，为安置 PLC 信号接入系统，最好拆除断路器控制面板，从而可以将 PLC 信号耦合至连接建筑物插座的不同的走线上。如果真地需要这样做，那就要获得电力网管理单位的授权并由专业电力工程师对电力网络进行局部的改造。

图 11.5　PLC 设备在电力线各相上的耦合方法

电力网络上电力线之间存在互感现象（尤其是在断路器控制面板附近，电力线之间的距离很近），所以下面的方法可以将 PLC 信号接入电力媒介。

1）PLC 信号感应到一根线路（单相或零线），并与其他各条线路感应。

2）PLC 信号同时感应到多条线路上，同时与零线互感应。

3）PLC 信号感应到每条相线，并通过三转一的 TV 分路器连接。互感现象将

在 3 条相线与零线之间发生。

11.3.3　安放设备

PLC 设备在电力网络中的安放位置直接影响 PLC 信号在房屋中各种线缆上的传输效果。因此，选择好位置以便安装最多的插座就显得尤为重要了，如图 11.6 所示。

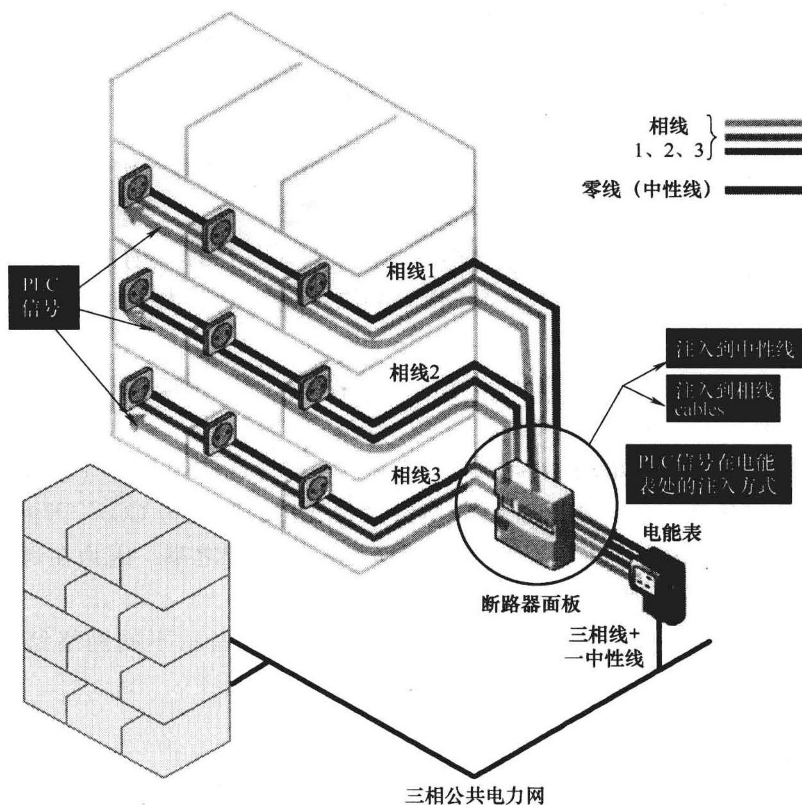


图 11.6　在电力分路器插入 PLC 信号示意图

断路器面板的位置在电力网中很重要。因为其可以看成网络中的集线器，所有的线路都通过它续接从电能表处进来的电能。因此，这个电力集线器也就是 PLC 网关设备的理想位置，它既连接企业的以太网又连接电力网，将以太网的帧信息转送到各种插座上的 PLC 设备上。

另外，重要的是一定要复现房屋的电力线图，以便了解电力网络的拓扑图，各相电路的配电情况等（三相交流电的情况下）。

11.4 选择网络结构

如第 3 章和第 10 章所述，根据所用的 PLC 技术，可供选择的网络结构有几种。

在点对点的拓扑结构（HomePlug 1.0 或 Turbo）中，充当以太网和电力网络之间网关的 PLC 设备在电力网中没有特定安放位置。这种网络结构适用于 LAN，在这一结构中，LAN 通过有线的以太骨干网相连接。由于每个设备都处于网络的同一层，因此需要注意不要将电力网络上的 PLC 设备隔开得太远（譬如可以每一相邻的房间放置一个设备）。

在主-从模式网络结构（DS2 或 Spidcom）中，主设备在网络中具有位置优势并且必须要能够显示网络中的各种 PLC 从设备的信息。这样一来，断路器控制面板再一次成为一个理想的中央位置，以便将 PLC 信号传输到电力网中各个主要的插座上。这个中央位置可以选在尽量靠近以太 LAN 设备的技术机房中。

在中心式网络结构中（HomePlug AV），包含的设备主要是 CCo（中央协调站）和 STA（工作站）。每一个 AVLN（AV 逻辑网络）中只有一个 CCo 来管理 PLC 网络中的 PLC 链路。HomePlug AV 规定，在网络中位置最好的设备（也就是能够看到所有 PLC 设备者）因其得天独厚的条件而会被自动定义为 CCo。因此，将 CCo 设备放在电力网最中心之处（断路器控制面板）是明智之举，因为在那里可以显示 HomePlug AV PLC 网络中的所有 STA。

在本章末尾，将就各种不同的网络应用的实例，展示不同网络结构的选取情况。

11.5 安全参数

与第 10 章一样，正确配置 PLC 网络密钥是极其重要的，其目的就是为了让不怀好意之人无法访问网络，续接电力线上的数据帧的传输。

这里特别说明一下，由于 Wi-Fi 的传播是在空中进行的，因此有可能被窃取；然而 PLC 技术通过有线媒介进行传输，因此那些试图通过重现信号数据帧来接入 PLC 传输媒介的行为就变得越发困难。

在企业网络中，有必要检查接入到因特网的防火墙配置是否正确，看看各种企业网络相互之间是否正确隔离，以保护彼此之间的数据安全。下面各节将就以实现这个目标为主线进行介绍。

11.5.1　安全拓扑

有一些极端的办法可以保证 PLC 企业网络的安全，比如，将整个 PLC 网络完全独立于现有以太网进行安装，或者在 PLC 网络和现有以太网之间加接入保护。

图 11.7 展示了第一种解决方案。就时间开销和设备购置情况来说，完全独立于现有以太网来安装 PLC 网络是很昂贵的。此外，企业将会发现需要管理两个因特网连接，两个 DHCP 服务器等，这样的管理模式更加费时。

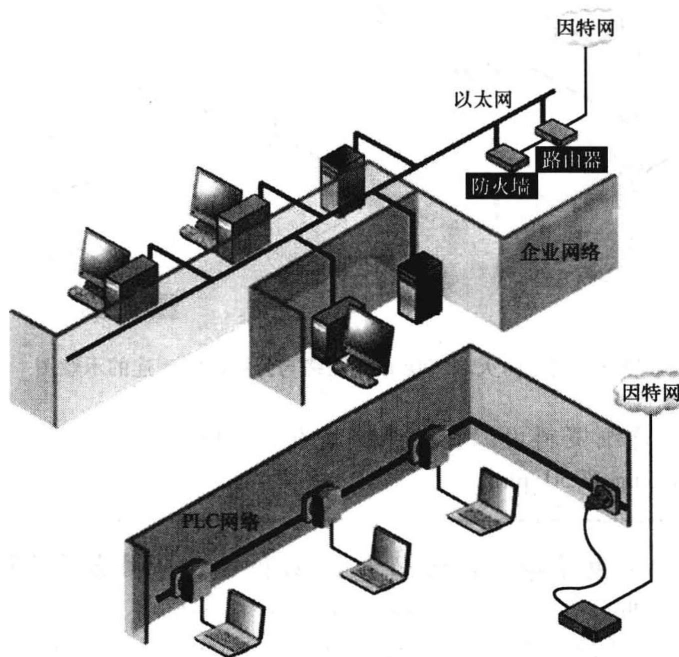


图 11.7　一个未连入公司网络的 PLC 网络结构示意图

图 11.8 展示了第二种解决方案。通过防火墙确保因特网安全连接的方法也用在了 PLC 网络和企业网络连接的安全保障上。

AsokaUSA 公司建议开发出一种交换机来管理不同的 HomePlug 1.0 和 Turbo PLC 网络。由于 HomePlug1.0 和 Turbo 网络在同一个时间仅仅支持一个网络密钥，因而这些网络不能同时属于同一个 PLC 网络。

进一步讲，如果使用相同的密钥，在同一个电力网络中，多个 HomePlug1.0 和 Turbo 的 PLC 设备不能相互区别。将这些设备隔离开来的唯一办法就是在每台设备中输入一个不同的密钥，将一个 PLC 设备当作网关，负责管理所有的网络密钥。

AsokaUSA 公司的 8950 交换机具备这项功能，可以同时管理 253 个 PLC 设备密钥和 1024 个用户。

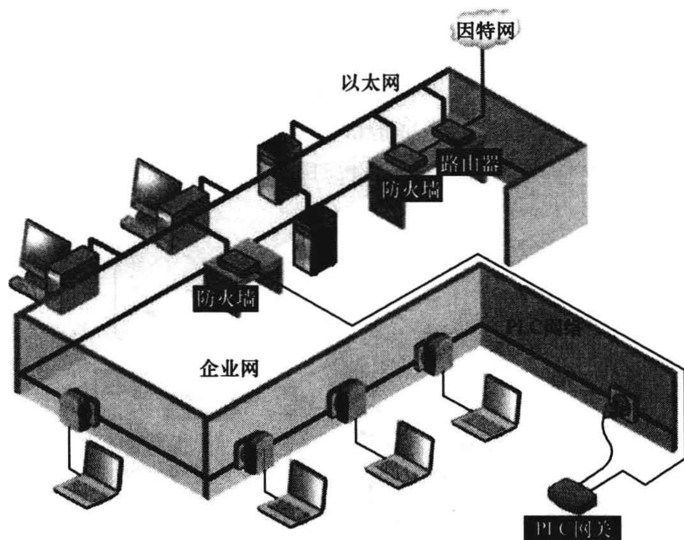


图 11.8 通过防火墙实现 PLC 网络与公司网络相连的示意图

这款产品的详细资料可以在这个网址获取：http://www.asokausa.com/products/commercial/plug_8950.php。

在 HomePlug AV 网络中，管理多个 PLC 网络，隔离各个 PLC 客户端

在那些 HomePlug AV 能提供但 HomePlug1.0 和 Turbo 不能提供的所有功能中，一台设备管理多个网络密钥的功能，使得 PLC 网络能够用多个网络密钥配置中心 CCo 设备，并且为其他每一个 PLC 设备都配置单独的网络密钥。这样每个设备之间彼此不可见，它们只能看见作为 PLC 网络中第二层网关的中心设备。因此，可以建立一种 FAI 结构，该结构中的每个组成部分仅能够访问因特网，而不能够接入到本地电力网络中的其他设备。由于其灵活性，稍加修改，这种 PLC 网络就可以让网络中的设备以同一个 IP 地址访问因特网。

PLC 安全配置

企业网络的安全性本质上是根据网络信息的搜集和网络攻击源头的检测而定的。

PLC 网络安全的重点在于正确地配置网络密钥，以优化电力网络中数据交换的加密措施（HomePlug 产品中，网络密钥必须是 20 个以内的大小写字母和数字）。

依照不同 PLC 设备的制造商以及不同的 PLC 技术体制，可以或多或少的配置一些高级安全功能。表 11.5 总结了各种 PLC 技术的重要安全功能。

表 11.5　PLC 技术的安全功能

PLC 技术		安全功能
HomePlug	1.0，Turbo	NEK（DES 56 位）
	AV	NEK，NMK，DAK（AES-128 位 + 密钥轮回）
	AsokaUSA	NEK，根据连接到 PLC 网络上的设备的 MAC 地址和 IP 地址过滤，在 HTTPS 配置接口密码
DS2		交换主从密钥，MAC 和 IP 地址过滤，在 HTTPS 配置接口密码
Spidcom		交换主从密钥

11.5.2　虚拟 LAN

顾名思义，虚拟 LAN（VLAN）就是用来定义虚拟局域网。这项多年前基于 IEEE802.1Q 标准的以太网技术使得同一个以太网中的多个虚拟局域网可以共存。

大部分企业的交换机采取这样一种方案，将 PLC 网络嫁接在现有的以太网之上。通过创建两个虚拟局域网，一个是以太网，另一个是专用的 PLC 网，这种方案就能形成一种如图 11.8 所示的拓扑结构，其中的各个网络互相之间通过防火墙隔离。

PLC 虚拟局域网是基于多个网络密钥（HomePlug 技术中的 NEK）的需求，或者是不同技术网络的需求（比如 HomePlug 网和 DS2 网）而产生的。HomePlug 技术支持 VLAN 标签的传播，VLAN 标签能够在企业以太网的交换机上得以配置。

11.5.3　虚拟专用网

和 PLC 家庭中的一样，虚拟专用网（VPN）是确保 PLC 企业网络安全的最可靠保障。为此，VPN 是基于客户端—服务器结构进行架构，其中客户端是连接到 PLC 设备上的工作站，服务器是专用计算机。

因为这种方案在第 10 章中已经详细描述了，我们在此不再赘述。虽然工程项目已经竣工，FreeSWAN 仍然是可供参考的 VPN 开放源代码的解决方案。详情请参考这个网站：http://www.freeswan.org。

11.6 安装和配置 PLC 中继器（桥）

如前所述，PLC 信号在电力线上进行传播，线路电阻和连接在电力网络上的电力设备所造成的电磁干扰，会对 PLC 信号造成严重衰耗。为了在整个房屋中解决这个损耗问题，获得最优和全面的 PLC 信号覆盖，可以安装一种叫“中继器”的设备，将 PLC 网络扩展到那些 PLC 信号损耗很严重的电力网络区。本节将举例说明如何配置中继器，扩展现有的 PLC 网络。中继器的概念和 PLC 网络段有关。

图 11.9 中的结构包括以下 PLC 设备：

1）PLC1 和 PLC2 是 PLT300 设备，按照 PLRP 模式工作，其可以通过以太网上的 Web 接口进行管理。

2）PLC3 是 PLT320 设备，按照 PRLP 模式工作，将 PLC 信号在电力网上进行放大接力。为此，PLC3 有两个 PLC 接口但无以太网接口，可通过 PLC1 和 PLC2 的 Web 接口管理。

3）PLC4 和 PLC5 是通常的无源 HomePlug PLC 产品，没有中继器时不能与 PLC1 和 PLC2 相连。

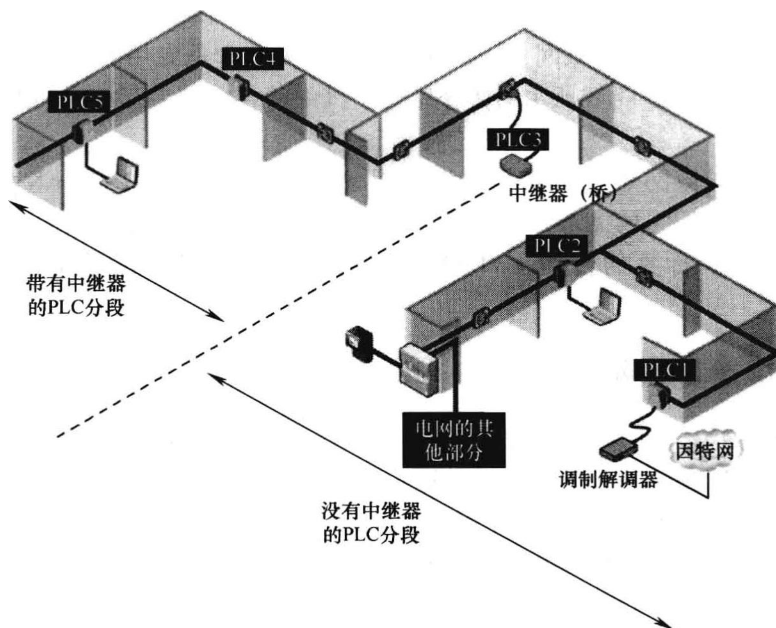


图 11.9 需要使用中继器的网络示例图

图 11.10 是网络逻辑图，它示意性地给出了各种不同的网络段互相连通形成的在整个电力网中完整的 PLC 网络。

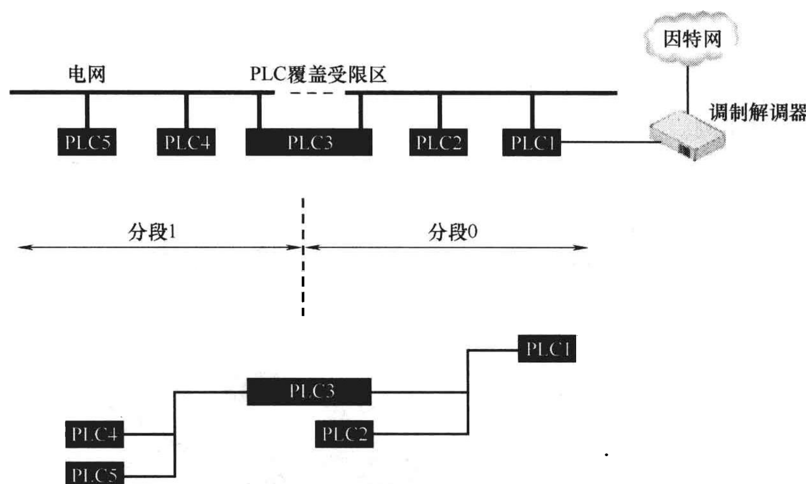


图 11.10　PLC 网络的两个中继区域之间的逻辑示意图

PLT320 的 IP 地址是 192.168.1.251。一旦配置 PC 恰好调整到同一个 IP 网络（比如 192.168.1.100），那么整个连接都可以使用相同的网络密码（默认值是 0）。

为了使工作的 Oxance PLC 设备变成一个中继器（桥），必须在 Oxance 的资源菜单的 PLT320 菜单中输入 MAC 地址，通过 PLT300 的接口连接到 PLT320 上，启动这个选项。下拉菜单中会显示出这个识别设备。这些标识符以 PLT 开始，以与 MAC 地址结尾相符的十六进制字符结束（MAC 地址为 0c000b0507e8 对应的设备标识符为 PLT_ 0507e8）。

因此，关键的操作是要在已配置好的设备中正确读取 MAC 地址，并且在资源下拉菜单中选中该地址，以便连接和修改它的配置参数。这样，我们就能选中 PLT320 了。

11.7　PLC 下的 VoIP

既然 PLC 网络在电力网络中可以视作以太网，IP 电话也就能够接入企业中。经过配置的电话可以接入 IP 类型的 PABX（专用自动交换机）。这个 PABX 可以续接源自 IP 电话的 SIP（会话发起协议）数据流，并且作为接入 STN 的网关（即使用模拟技术的电话网）。

Michael Spencer 公司开发的免税版的 Asterisk 工具可以在这个网址下载：http://www. asterisk. org。它可以安装在企业网络中，管理 PLC 网络上的 IP 电话。自 Asterisk 项目之后，Digium 公司开发了一系列基于 Asterisk 应用的服务和产品。

这种方案的优点是在整个电力网上移动 IP 电话成为可能。图 11.11 便给出了这样一个结构图例。

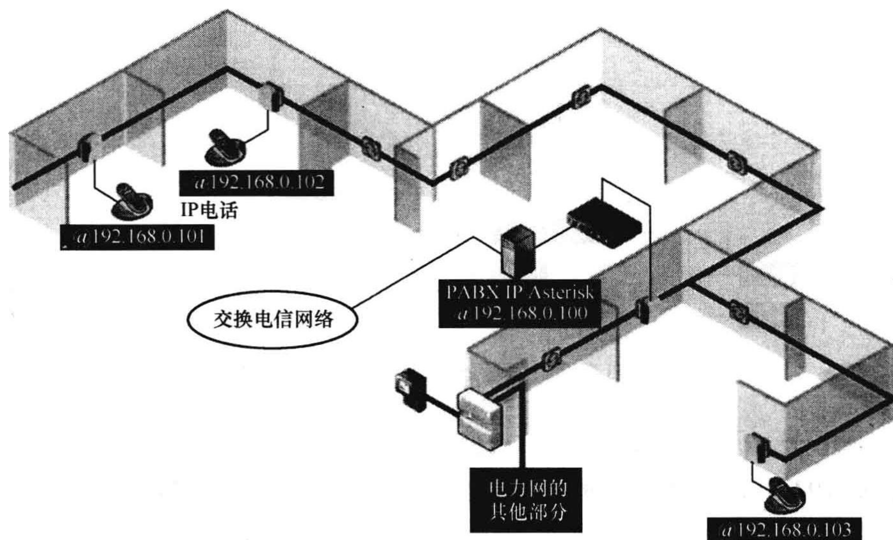


图 11.11　PLC 网络中 IP 电话的基础架构

11.8　PLC 在酒店中的应用范例

一家酒店想安装一个多功能计算机网络，来为它的顾客提供多种多样的服务，因此决定安装一个 PLC 网络。图 11.12 示出了一个酒店网络的结构图，在该结构中，两栋楼共用一个电能表，各用一个分路器。

对于这两栋房子，酒店经理希望有以下功能：

1. A 栋

1）每个客房能安全保密的接入因特网。

2）餐厅收银机接入网络并且将它连入酒店信息系统。

2. B 栋

1）会议室 1，建立一个基于 PLC 的本地以太网，使得网络中的计算机可以相互连接并且能够与因特网安全连接。

2）会议室 2，建立一个与会议室 1 相同的网络，但要求两个会议室的网络间的数据能够安全交换。

3）能够访问公共因特网并且向客户开放的两个房间。

4）报告厅具有 PLC 网上的 IP 视频会议功能。

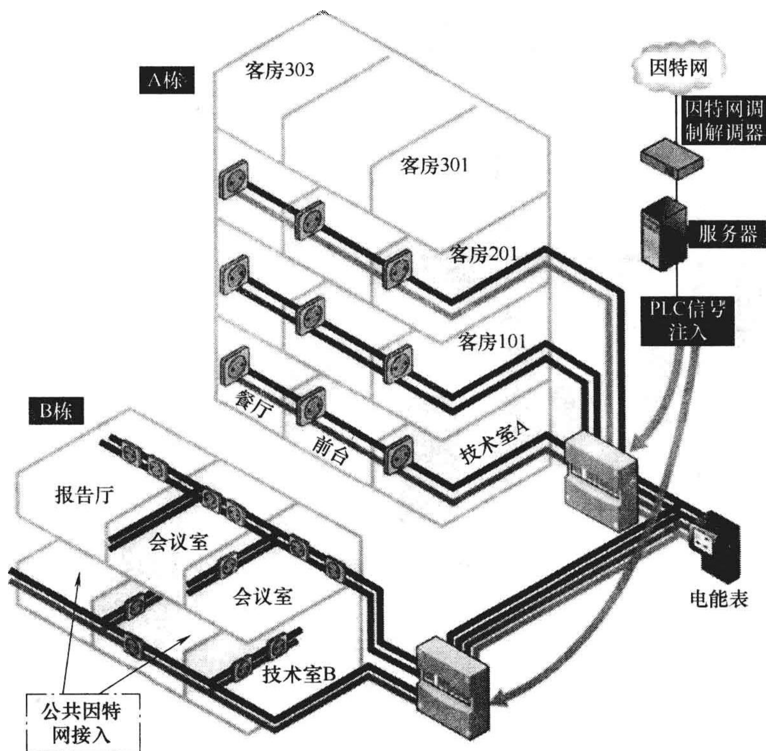


图 11.12　酒店 PLC 网络结构

网络安装

安装网络，需要正确绘出连接两栋房子的逻辑网络以及两栋建筑之外的逻辑网络。

如图 11.13 所示，在这个网络结构中需要考虑以下网络单元和参数：

1）安放和配置各种 PLC 网关和 PLC 信号注入器；

2）酒店的因特网接入；

3）各种 PLC 设备的网络密钥，不论是否独立；

4）两栋房子之间的网络链路。

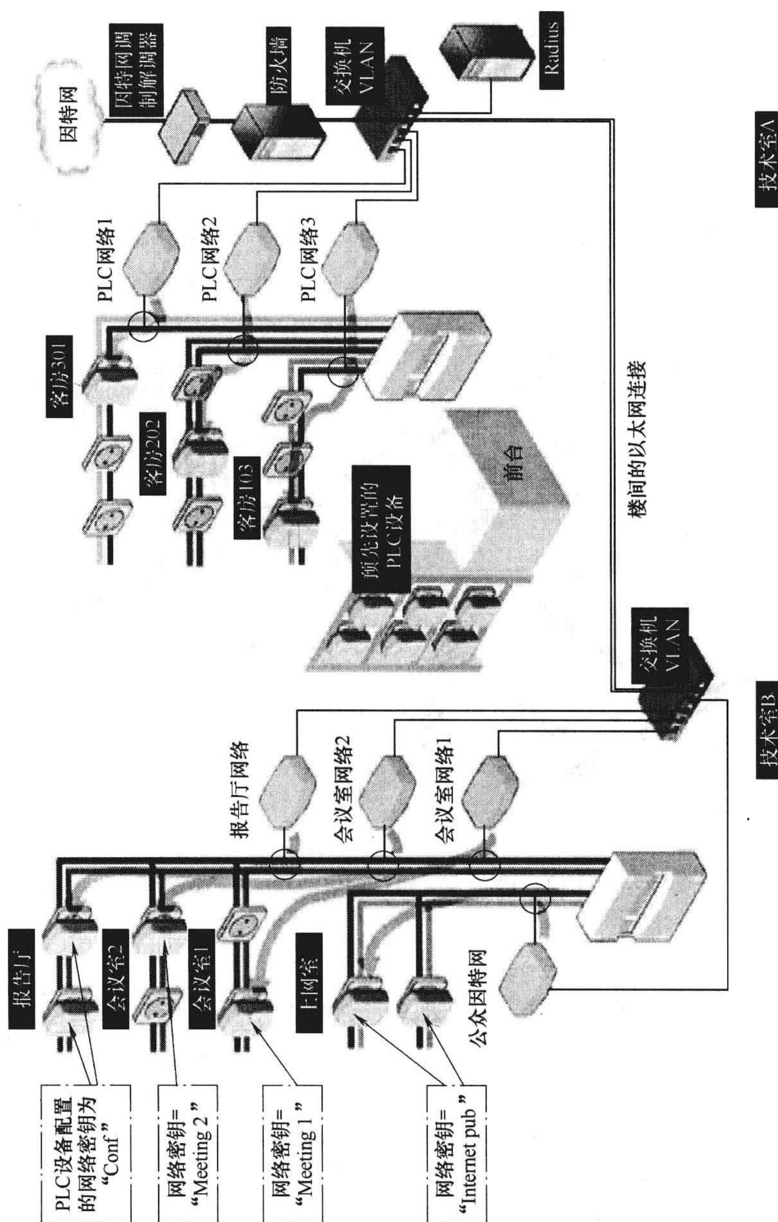


图 11.13 完整的酒店 PLC 网络结构

图 11.14 给出了这个网络需要安装的所有逻辑结构。由于我们想获得良好的吞吐量性能，保持稳定的服务以避免 B 栋的 IP 服务等级下降，这个逻辑结构中采取了有线的以太网来连接两栋房子。

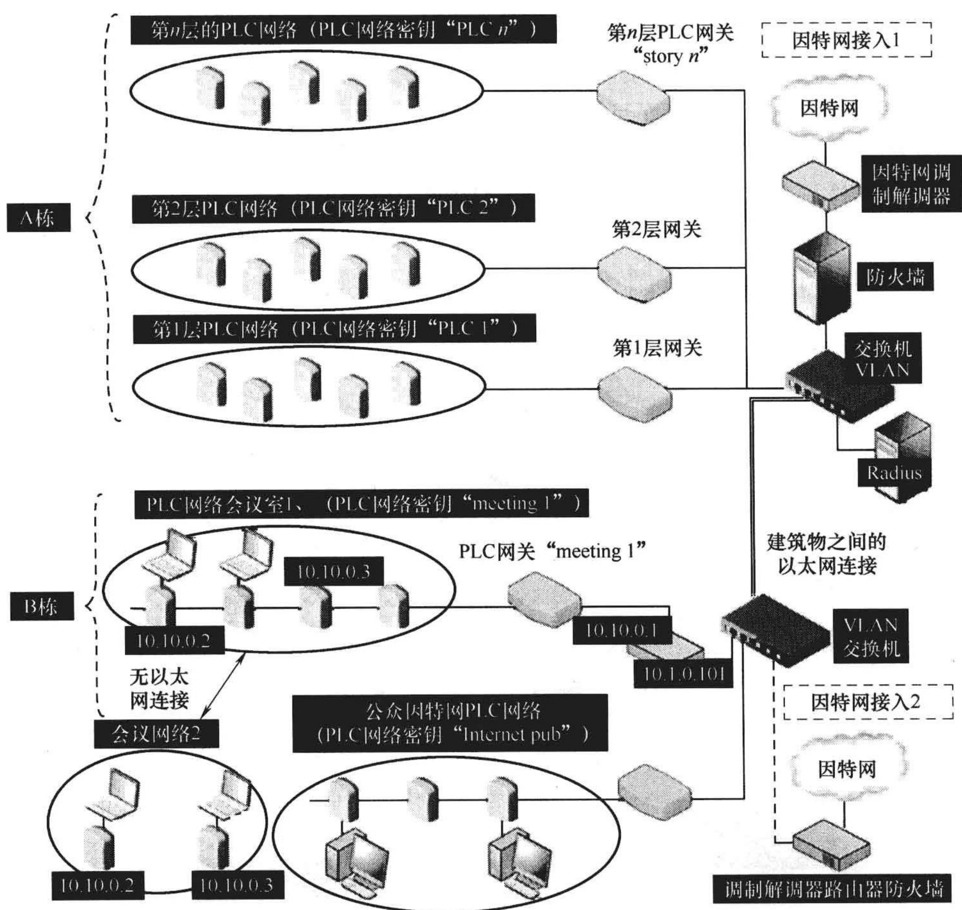


图 11.14　酒店 PLC 网络完整的逻辑结构图

为了尽可能地隔离各个 PLC 网络，重要一点是将这些 PLC 网络放在不同相位的电力线上（三相电缆和零线），而且一定要为每个设备配置不同的网络密钥。就安全性而言，可以考虑安装 RADIUS 服务器，对 PLC 网络客户端进行鉴权。

图中画出了接入信息系统的 PLC 网络连接（特别是酒店客房的因特网接入）和为会议室配置的 NAT 路由器（用来保护客户电脑的安全），以及具有管理多个 PLC 网络能力的企业网络。

酒店各楼层 PLC 网络

酒店可建议客人通过租用连接在客房插座上的 PLC 设备，在客房里面访问因特网。这种接入方式必须以一种鉴权、安全和保密的方式来实现。因此，在酒店接待处安装的 PLC 设备需要事先配置好，以便连接到各楼层的 PLC 网络。

由此所引起的技术问题是，HomePlug1.0 和 Turbo 的规范要求在一个 PLC 网关之后的每一 PLC 网络只能连接 15 台 PLC 设备。图 11.15 中显示，酒店各楼层网络中的 PLC 设备超过 15 台，而且是分布在酒店的 22 间可以接入网络的客房中。PLC 信号从楼宇的断路器控制面板处注入。考虑到楼宇高度可能较高，因此酒店在每层楼都安装了楼层 PLC 网关，并在每层楼之间使用以太网连接。

使用 AsokaUSA 公司的 8950 产品，通过添加“分段”的方式，PLC 网络可以突破以上的网络设备数量限制（即一个 PLC 网络内最多 15 台 PLC 设备这一限制）。

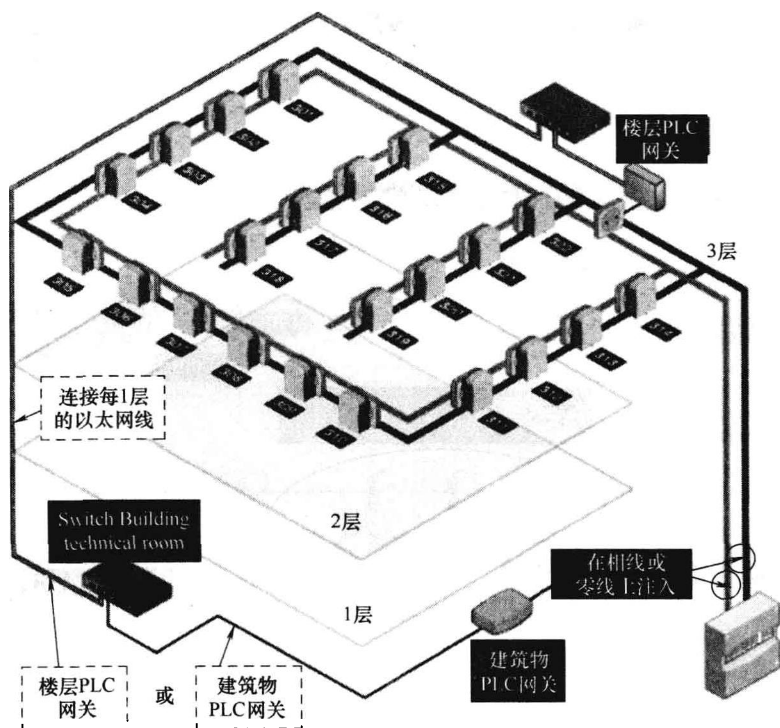


图 11.15 超过 15 个设备的 PLC 楼层网络示意图

对于图 11.15 所示的 22 个客房，只需要建立两个分段（一个分段包含 15 台设备，另一个包含 7 台）就可以满足本楼层的所有需要。

图 11.16 为基于 AsokaUSA 8950 设备配置的 PLC 网络结构，该设备可以管理带有 15 个 PLC 设备的 3 个段。

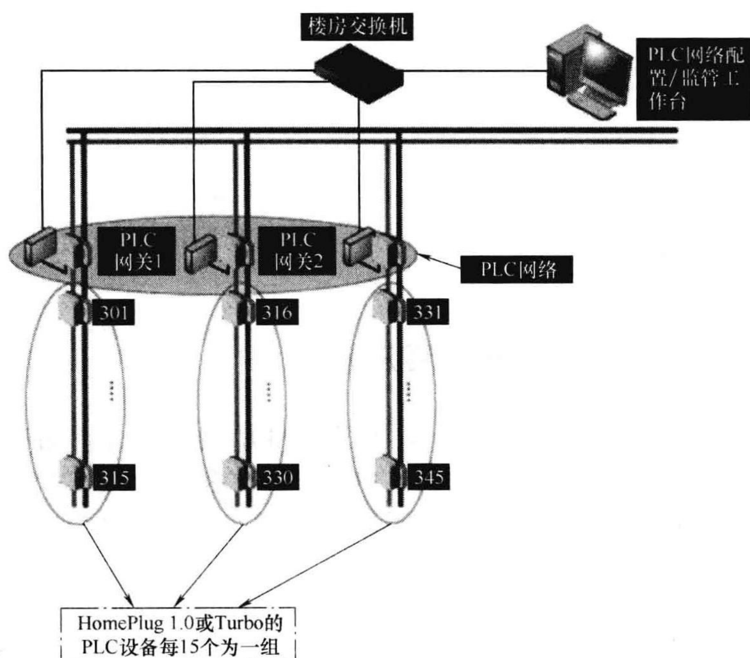


图 11.16　有多个 PLC 区域的楼层网络结构图

各电脑加密访问因特网

如图 11.17 所示，PLC HomePlug 1.0 和 Turbo 网络的缺点之一就是它们存在着媒介共享，在 PLC 网络设备之间，甚至 3 个客房之间，可能还存在着网络连接。

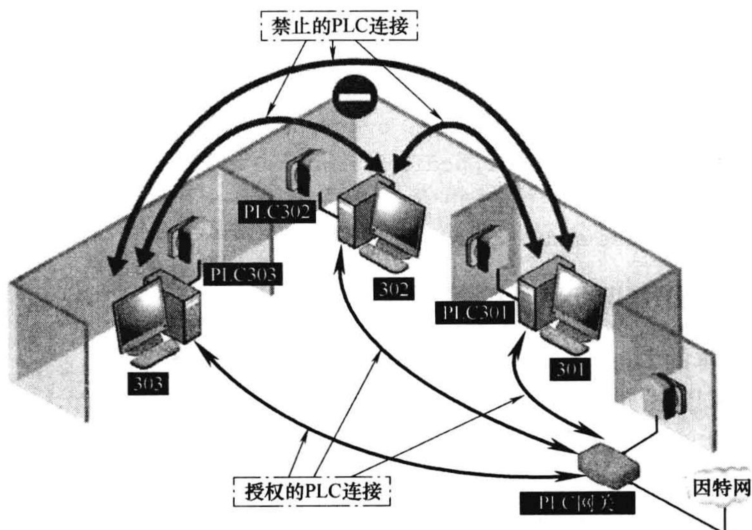


图 11.17　各电脑的接入因特网安全性示意图

不过，使用 AsokaUSA 的 PlugLAN 8950 设备，就可以在 PLC 网络的电脑之间设定 PLC 设备的数据过滤规则，保证数据可靠性。

假设客房网络的地址是 192.168.0.1/24，通过 HTTP 接口，在安全菜单，选择数据过滤子菜单，选中编辑框，就可以设定这个规则。当然，新的规则必须设定准备过滤的所有发起访问的电脑的 IP 地址以及被访问电脑的 IP 地址。

上述规则还必须阻止 192.168.0.1/24 网络中任意两台各计算机之间的双向 IP 数据流，此外还需要新增一条规则，对流向网络之外的双向数据流进行鉴权[⊖]。

11.9 Linux 下配置 DHCP 客户端

现在，不管是服务器端，还是客户端，Linux 越来越多地应用于企业网络中，因此，对于专业网络的管理员来说，学会在 Linux 下配置 DHCP 客户端就显得非常重要了。

在开始配置 DHCP 客户端之前，需要确认一下，以太网卡是否在 Linux 下正常运行。如果不行，需要重新安装驱动程序。

Linux 下，有两种广泛应用的 DHCP 客户端：dhclient 和 pump，所有的 Linux 发布版本都支持这种客户端。

输入 dhclient eth0 或者 pump eth0，可以对 DHCP 客户端进行手动配置。修改 /etc/pcmcia/networks.opts 文件，可自动将客户端设定为 eth0 网络接口。

在操作界面中，只需要输入 ifconfig eth0，就可知道网卡参数的状态是否设定好。如果网卡没有被 DHCP 服务器配置好，就不会显示 IP 地址：

```
# ifconfig eth0
eth0 link encap:Ethernet    HWaddr 00:02:2D:4C:05:B8
     inet addr:10.0.0.2     Bcast:10.0.1.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
     RX packets:1 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:100
     Interrupt:3 Base address:0x100
```

11.9.1 配置 DHCP/NAT 服务器

大部分版本的 Linux 都支持一款叫 dhcpd 的 DHCP 服务器。

配置 DHCP 服务器，需要创建一个 dhcpd.conf 配置文件，以下是一个 dhcpd.conf配置文件的例子：

⊖ 这一段话的意思是：通过设定相关的规则，阻止在本地 PLC 网络中未经授权的网络连接，并且阻止这些连接的双向数据流通过网关（交换机）等流出本地 PLC 网络。——译者注

```
Subnet 10.0.0.0 netmask 255.255.255.0 {
Range 10.0.0.2 10.0.0.50;
option routers 10.0.0.1;
option domain-name-servers 10.0.0.60;
default-lease-time 1000
max-lease-time 3600
}
```

1） Subnet 用于定义网络 IP 地址段；
2） netmask 定义子网掩码；
3） Range 定义了 dhcpd 服务器提供的地址范围。
4） option routers 定义默认网关的 IP 地址；
5） option domain- name- servers 定义 DNS 地址；
6） default- lease- time 定义默认失效时间，在这里为 1000s；
7） max- lease- time 定义最大失效时间。

输入下面的命令，就可以打开网关，启动 dhcpd 服务器：

```
# dhcpd eth0
```

这里 eth0 是连接到网关的以太网卡。

也可以在/etc/rc 文件夹中创建一个 script 脚本，并且输入以下命令，启动 dhcpd 服务器：

```
/usr/sbin/dhcpdt eth0
```

11.9.2 NAT

NAT（网络地址转换）是将多台计算机以同一个 IP 地址连入因特网的技术。NAT 至今仍用来弥补网络中可用的 IP 地址数量较少的不足。

若一个 PLC 网络如图 11.18 所示，其中有一个 PLC 调制解调路由器连接到因特网。

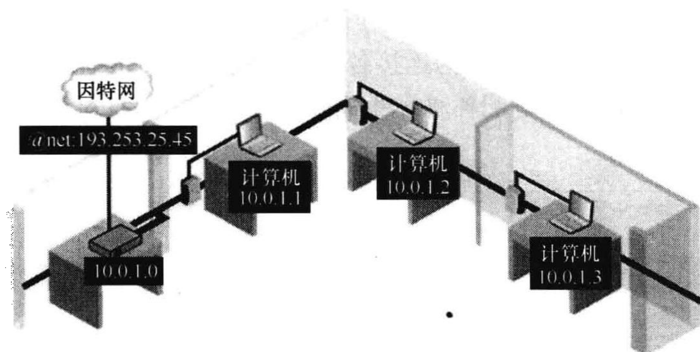


图 11.18 PLC 网络连入因特网

那么只有当因特网调制解调器或者网络中其他设备具有 NAT 路由功能，并且连接到因特网上时，PLC 网络中的计算机才能连通因特网。

NAT 路由功能可以让多台没有路由功能，只有内部专用地址的计算机，使用同一个路由地址访问因特网。

当一台计算机发出的数据不是送往局域网内部时，NAT 路由器——在本例中就是因特网调制解调器——将发送者的 IP 地址代替为对外的，由 ISP 提供的广域 IP 地址（图中的@ net 地址），同时因特网调制解调器将这次连接信息（发送者的 IP 地址、所使用的协议）存入翻译表中。

当因特网调制解调器收到来自因特网的数据时，借助存在表中的信息，通过比较接收到的数据类型，可以检查数据接收者和翻译表中的信息。找到数据接收者后，@ net 的 IP 地址就被替换成数据接收者的内部 IP 地址。通过这样的办法，所有的计算机都可以使用同一个 IP 地址访问因特网。

NAT 可以通过地址配置情况过滤数据包，避免外来的攻击。如果这些连接没有被 NAT 服务器所事先初始化，NAT 路由器就不会处理这些外来的数据包。

NAT 配置

与 DHCP 服务器不同，NAT 配置取决于所用的核心版本，究竟是 2.2 还是 2.4/2.6。在这些情况下，作为 DHCP 服务器，打开网关后，可以手动启动 NAT，或者在文件夹/etc/rc 中写入 script 脚本，在启动网关时区分 NAT 的运行。

不论使用何种内核，必须用 vi 命令修改/etc/network/options 文件，比如，修改参数 ip_forward = yes。

对于 2.2 内核，ipchains 命令可以管理 NAT：

```
/sbin/ipchains -A forward -I ppp0 -s 10.0.0.0/24 -j MSAQ
```

其中，ppp0 是连入因特网的接口。

对于 2.4 和 2.6 内核，就要用 iptables 命令管理 NAT

```
/sbin/iptables -t nat -A POSTROUTING -o ppp0 -s 10.0.0.0/24 -j MASQERADE
```

其中，ppp0 是连入因特网的接口。

如前所述，PLC 网络可以视为连接各个 IP 终端的第二层基础（以太网）。所以，连接到网络中设备的 IP 配置通常可以在所有 IP 网络中看到（IP 寻址、DHCP、NAT 功能等）。

第 12 章　PLC 在社区中的应用

近年来，因特网接入提供商着力研究开发了其建议的高吞吐因特网接入技术，即提供了较高的吞吐速率，也为数量不断增加的消费者提供了新的可供接入的媒介（诸如电话线、电视电缆、无线电等）。

在这个框架下，特别是在世界上的一些国家中，电力网络看上去更有希望通过整个大厦或者公寓的插座，将因特网信号按照尽可能短的路线传送到目的终端。

使用公共电力网络作为通信的媒介，特别是将因特网信号传输至最终用户具有明显的优势，因为电力网络到处都有。但是使用这样一个原本用来输电和配电的媒介作为通信的媒介，的确需要小心。

本章将介绍把 PLC 网络部署到整个社区的每一户时需要引起注意的一些制约和设备选取的事项。这种类型的 PLC 网络结构已经被一些无线通信运营商应用。

12.1　社区的电力网络

正如我们在前面章节提到的，电力网络从广义上讲可以看作若干连接在一起的不同电压、不同用途、不同管理人以及不同安全级别的子分支网络。

首先举一个例子，有一类子分支网络，它们是从纵跨全国的源自主要发电厂的 EHV（超高压）线路上分出，经过不同的社区，到达建筑物（如房屋、公司等）的插座上去，这类子分支网络在美国受 FERC 管理，而在法国受 CRE 管理。

图 12.1 示意性地说明了不同的子分支网络，同时配上了它们各自不同的电压情况以及相关的传输线的类型，此外，还说明了所连接的直到电能表下游的个人电力网络（电能表用于建筑物和公共电网之间的电力连接）。社区电力网络指的是从 HV/MV 变压器到社区建筑物的电能表之间的网络。

这些电力网络的子分支网络往往不尽相同。一方面，作为高压电力网络的组成部分，社区网络的所有者所布设的线缆、电塔、基础设施等各有特点；另一方面，低压电力网络电力设施以及网络的使用、供应、服务和组成等往往也都有各自的特点。

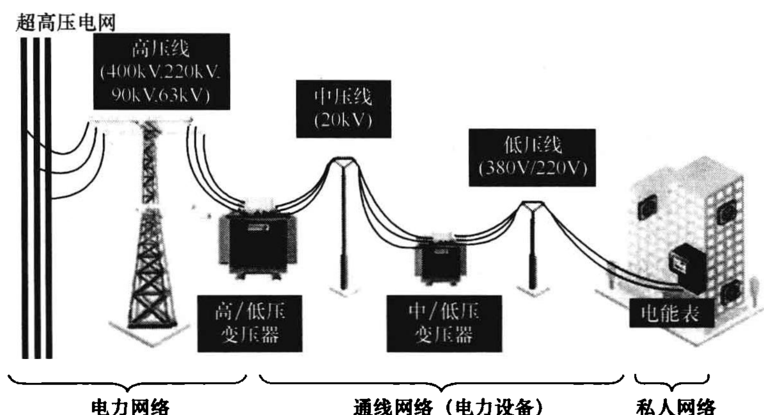


图 12.1 电力子分支网络的结构

图 12.2 展示了作为低压电力网络和公共电力网络连接点的电能表所担负的双重责任。在研究 PLC 网络时，理解这一点十分重要，因为 PLC 设备必须安装在电力网络的不同部位以便使 PLC 信号可以从 IP 网络连接点传输到公共电力网络用户的插座上。

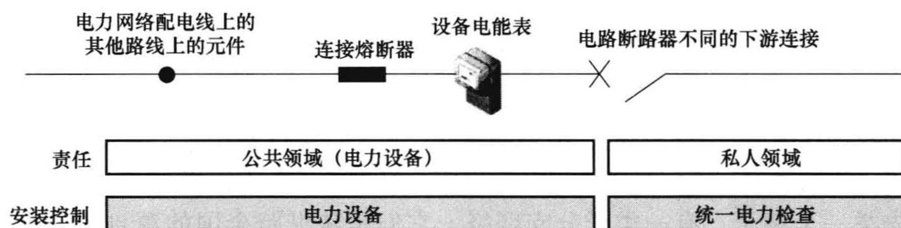


图 12.2 电力配电网络的双重责任示意图

12.1.1 电力网络运营商

作为一个电力网络运营商，无论是地区的、全国的，或是国际的，无论其电力网络遍及有限的地理区域，或是遍及整个国家，PLC 网络的布设，使得它们就像一个因特网接人的接入服务提供商，成为一个电信运营商。这样，电力网络运营商要在电力网络的框架下担负起通信网络建设和管理。电力网络的安全规则与那些同轴线缆，有线电视或者光纤通信网络是存在不同的。

对于区域电力网络设施（村庄社区、小镇、建筑物众多的区域、私人企业联合会等）的管理，PLC 是将这些处于空旷地带的地区性机构连接到因特网上去的最好选择。

不论是实验性质的，还是商业性质的，PLC 网络技术的最新研究均表明该技术

可以有效地为家庭提供因特网接入服务，获取因特网带来的便利。PLC 技术的开发往往都是建立在当地电信运营商的基础上的，充分利用了各运营商现有的成熟技术（例如 BLR、Wi-Fi、Mesh 网络技术等）的网络结构。

有些时候，电力公司往往喜欢将他们自己局限于发电、输电以及较为熟悉的配电业务中，而不愿意将自己视作可以向有着三千万左右电能表的网络提供通信服务的运营者。而且，这往往是当地行政上针对每一个电力企业和电网系统专项规定产生的结果。

12.1.2　电力网络的拓扑结构

若干建设方面的原则决定了电力网络的实施采用“分布”式，也就是说电力网络连接到主要的高压（即 HV）网络上，通过向用户的电能表提供电力来实现对社区建筑物的供电。

首先，根据建筑物的密度和地理环境因素，可以将中压（MV）和低压（LV）电力网络分成 3 类，即乡村型、半城市型和城市型（见图 12.3）。这 3 种电力网络包含以下特征元素。

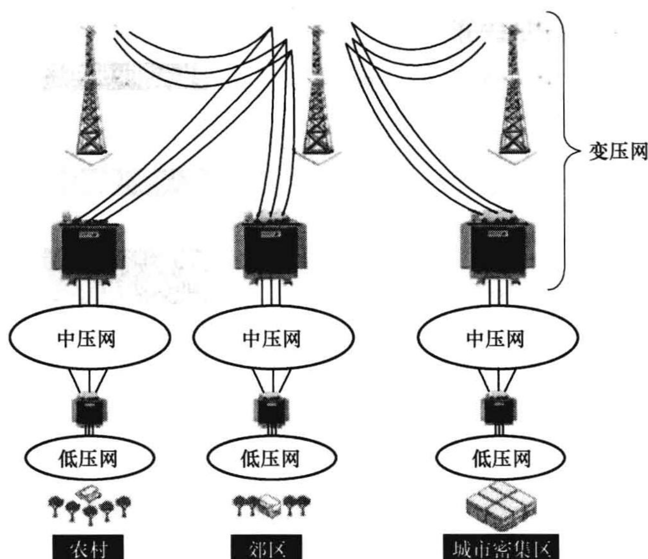


图 12.3　MV 和 LV 电力网络

1）网络拓扑；
2）铁塔距离；
3）变压器和不同的供电电能表之间的距离；
4）在中压/低压（MV/LV）分配变压器之后的电能表的数量。

对于每一类型电力网络，中压（MV）电力网络都会采用以下 3 种拓扑结构：星形（Star）、环形（Ring）以及网络型（Mesh）。目前应用最为广泛的是网络型，这种拓扑结构能够保护整个电力网络，免受网络个别节点故障的影响。如果某一点出现故障（譬如说短路）造成电力网络受到影响，其他电力线路可以接管这个故障点，因为网络型拓扑能够具有备份功能。换句话说，整个电力网络的每一个节点都不是由单一电力线路供电的。

12.1.3 中压网络的拓扑

在乡村地区，“树状”的星形网络拓扑应用广泛。在半城市（城郊）地区，“树状”的星形拓扑和环形拓扑在一些与高压网络的连接节点处也有使用。

在人口密集的城市区域，网络型拓扑结构广为使用，但实际上是采用加强型的星形拓扑结构来配置的。网络结构的好处就是能够在一条主要的供电线路断开时仍能够提供备份连接。图 12.4 ~ 图 12.6 说明了这些中压（MV）网络拓扑。

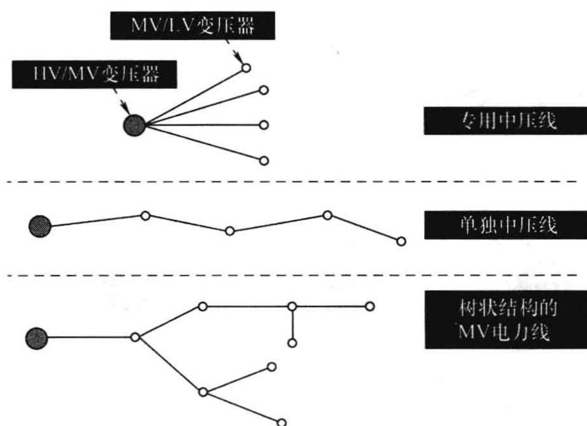


图 12.4 星形拓扑结构

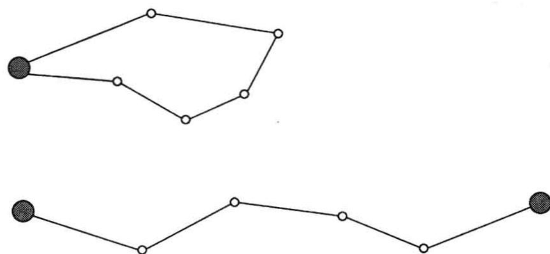


图 12.5 环形拓扑结构

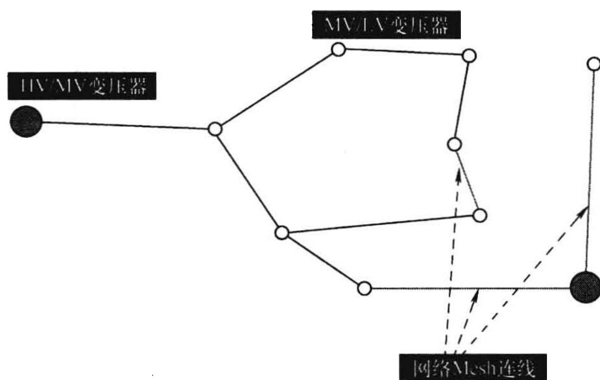


图 12.6　Mesh 拓扑结构

12.1.4　低压网络的拓扑

在很多国家，低压电力网络的拓扑结构是一个树状的星形拓扑结构，从而在一些电力网络的分支中形成网状。但是，这些网状连接还是比较少的，不足以将这种网络拓扑定义为真正的网状拓扑结构。

电力网络的建设规则决定了 PLC 的建设工程应当以获得最好的覆盖和向用户以及社区建筑物中的插座提供最好性能的 IP 网络为目标。

图 12.7 说明了一种具有社区电力网络中的代表性网络，该网络是从中压/低压变压器到不同低压网络的分支，向用户的电能表提供电力。

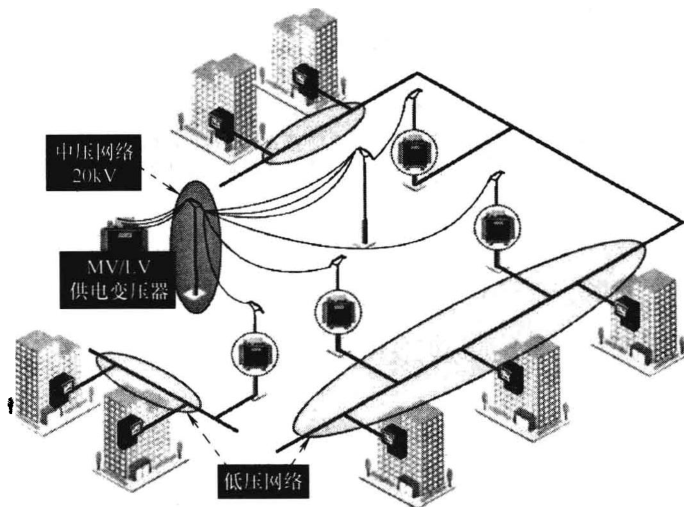


图 12.7　社区电力线配电系统示意图

如果我们仔细研究一下拓扑结构以及在稠密市区环境下的电力线分布系统的电力设备（例如住宅的电能表），我们就不难发现图 12.8 中所示的结构。该图详细介绍了从本地变电站到公寓的电能表这一电力网络的不同组成部分。用于将数据信息从变电站传送到公寓中的 PLC 从设备的 PLC 设施就工作在这一电力网络上的。

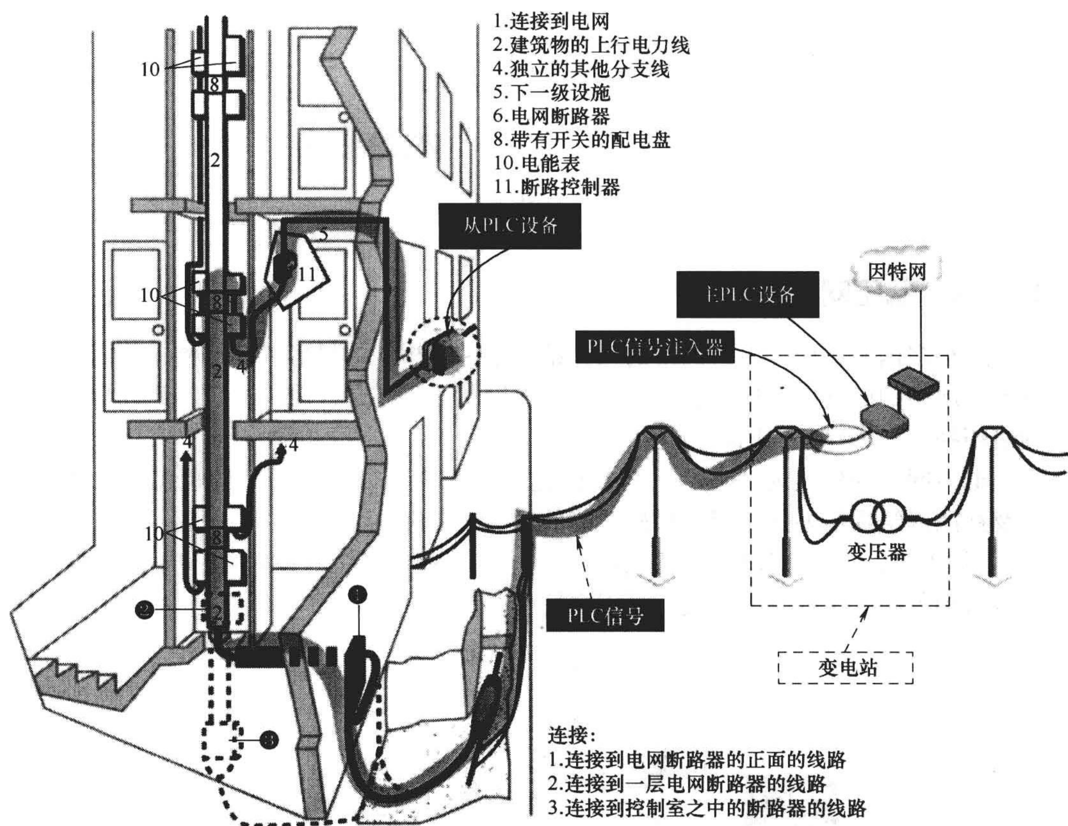


图 12.8 在密集城市地区的拓扑结构和电力设备

12.2 社区范畴的 PLC 网络的建设

在为一个社区建设安装 PLC 网络的时候，必须考虑一系列因素。首先，应当成立一个项目团队，与当局签署好协议（在协议中，社区应当明确定义好因特网和 IP 网络的需求以便确定技术规范书），并选定一个主要的工程承包方，明确工程量以及与当地电力设施的运行团队合作开展 PLC 基础设施建设。

这个主承包方团队应当由符合安全规范的电力工程师以及符合住户关于网络业务和电力设施建设需求的电信/网络工程师组成。

12.2.1　PLC 在网络结构中的位置

电信网络可以看成是一座巨大的金字塔，它由以下几个子分支网络组成（由顶至底）：

1）超大网络：该网络确保城镇和大陆之间的超高吞吐速率的网络连接，主要使用光纤连接，例如位于欧洲的欧洲主干网（Ebone）或者欧罗巴网（Europanet），位于东非的 Eassy，位于西非的 SAT-3/WASC，以及从北非到印度的 SEA-ME-WE-3 网络系统等。这些网络不能使用 PLC 技术。

2）交互式 POP（Point of Presence）骨干网：该网络将既有的众多超高吞吐速率的 IP 节点连接到大城市的数据中心，将既有的节点连接到因特网接入提供商的交换设备上（电话交换机、有线电视、卫星、Wimax、BLR、Mesh 网络等设备）。这个骨干网采用光纤连接，铺设在城市之间或者高楼林立的区域。以前，PLC 技术不能用于组建这类网络，但 HomePlug AV 和 HomePlug BPL 具备的吞吐能力在某些情况下可以成为这个网络的组成部分。

3）配电网络：主要用于连接因特网提供商的交换设备以及将用户连接到因特网和 IP 网络上。这些网络包含了能够为因特网接入提供商的交换设备几千米之内的用户使用的全部媒体。考虑到电力网络的拓扑能够到达全部的建筑物和社区建筑物中的每一个插座，因此 PLC 技术无可争议地成为了这种配电网络的理想应用技术。

4）局域网（LAN 或者称建筑物之间的网络）：通常是以太网或者 Wi-Fi 网络，它们有可能部分或者全部被 PLC 技术明显的优势所替代（如吞吐量、安全性、架设的便捷性以及插座的冗余性等）。

本章中所提及的社区中的电力线系统是通过构建一个能够使用 PLC 技术的配电网络，或者使用一种融合了若干种网络技术的混合网络来为社区中的各个建筑物提供高的因特网吞吐量。

图 12.9 展示了这种无线电通信网络的金字塔结构，通过这个示意图，说明 PLC 技术所处的 LAN 级别以及在社区情况下的配电网络情况。

12.2.2　电力网络对电力线结构的制约

假设一个国家的电力网络与它的邻国是不对接的，那么在考察这个电力网络的时候，低压电力网络对 PLC 网络的结构存在如下影响：

1）地理区域的影响。在一个居住区域、一个企业云集区（这里一般来说电能表的密度比较大）、或是一个工业园区（这里更多地需要 QoS 有保障的服务），电力网络的特性各不相同。

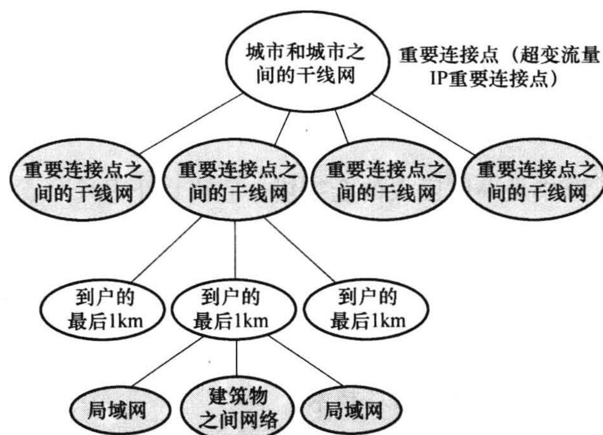


图 12.9　通信网络金字塔示意图

2）低压电力网络上的电能表数量的影响。郊区和高楼林立的市区的电能表的密度大相径庭。

3）电网的拓扑结构。电力网络包含电力环路，这些环路将变压器与终端有机地连接起来，环路的数量与所研究的区域息息相关。

但是，需要明确一点，如果我们注意到连接着若干国家电力网络的现有拓扑结构的不同的话，那么就会发现 PLC 网络面临着新挑战，此时，上述的一些制约就可以暂不予考虑了。

举一个例子：在美国，大城市郊外的房子星星点点，并且连接到 MV/LV 变压器上的电能表的数量屈指可数；不过在法国，这一数字却能达到平均 200 余个。在这种情况下，就不难理解，“变压器的远程控制与共享资源的用户数量”这一参数在欧洲就比在美国更具有制约性。

12.2.3　PLC 的结构

为了使得 PLC 技术在社区配电网络环境下提供因特网接入等服务，就要求 PLC 的结构与第 10、11 章中的结构有所不同，毕竟那两个结构是为了使用家庭、企业环境的。

社区中的低压 HTA 电力网络起自 MV/LV 变压器，连接至建筑物的电能表，是一个星形的拓扑结构。此外，配电网络需要在不同的 PLC 网络之间设置隔离措施，从而避免 PLC 网络用户与因特网之间传送的数据被窃取。

这就意味 PLC 的结构是一种主从结构。网络中的主设备：

1）监视、管理以及监督不同的网络设备；

2）确保每一个与因特网相连接的用户的安全和保密；

3）确保能够扮演网关的角色，从而连接到其他 IP 网络上去，特别是连接到社区其他可用的 IP 传输点上（卫星、IP-POP、光纤、BLR、WiMax、Mesh 等）。

图 12.10 展示了 PLC 结构的一个例子，在社区中，从 MV/LV 变压器连接到不同分支电路上的星形网络，从而构成了这个社区的 PLC 结构。

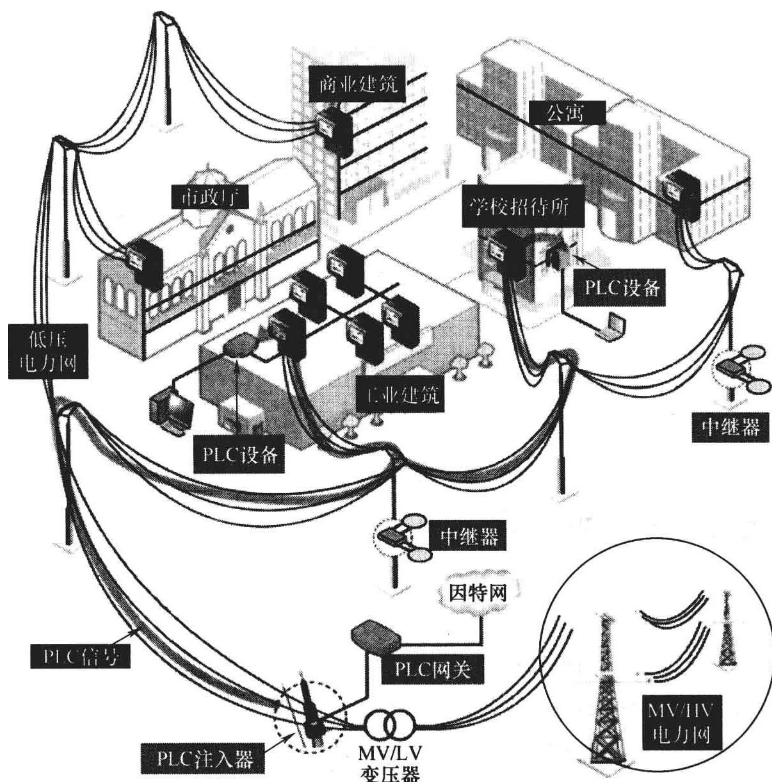


图 12.10　社区中的 PLC 结构示意图

这种结构的核心内容如下：

1）PLC 网关用于和其他 IP 网络相连。

2）如图 12.11 所示，在公众电网中使用 PLC 注入器。

3）在整个连接至用户的线路（可达 200～300m）中使用 PLC 中继器来提供连续的 PLC 信号。PLC 网络在本地管辖（即社区管辖）的优势在于电力网络比家庭或企业的 PLC 网络能更好地应对电网的干扰。

4）网关的位置在电网的变电站处，也就是在 MV/LV 或者 HV/MV 变压器所在之处，这样 PLC 信号可以在公共电力网络的星形拓扑结构的节点处被注入。

PLC 的这种分布式网络结构说到底是相当简单的，并且也没什么新鲜之处，这和家庭或企业的 PLC 网络是不同的。因为在家庭或企业网络中往往缺少电力网络

施工图，因此 PLC 网络的布设之前需要进行测试。

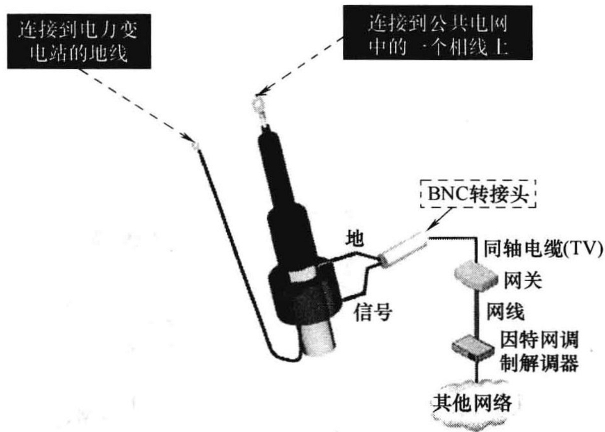


图 12.11 Eichoff PLC 注入器的连接器示意图

拿社区网络来说，电力部门已经掌握了需要的全部电器设备信息（电缆类型、电缆长度、每一电路支线上的用户数、变压器类型以及 PLC 中继器最恰当的位置等）。

12.2.4 电力网络方面的问题

在一个公共电力网络上安装通信设备，有关各方必须遵守一系列的安全规定，特别是那些关于电力设施的操作和相关技术管理内容。

对于我们关注的 PLC 网络来说，以下规定需要注意：

1）耦合设备和中继设备应当具有良好的电学隔离特性。

2）对于在电网上的操作，PLC 设备需保持一定的透明性。

3）PLC 设备必须由授权的人员进行操作。

有资格对电力网络进行操作的人员应当获得经专门机构认可的专业训练和认证。

表 12.1 就列举出了根据需要的操作不同（降压、断电或供电），从事电网工作的人员获得不同的授权所对应的不同技术课程。

表 12.1 电力授权

授权等级	降压		断电		供电	
	LV	HV	LV	MV	LV	MV
非带电操作	B0	H0	B0V	H0V	—	—
带电操作	B1	H1	B1V	H1V	B1T	H1T
管理人员	B2	H2	B2V	H2V	B2T	H2T

无线电通信设备的安装以及大多数公共电力网络上的电力设施的安装需要特别注意以下几方面的事项：

1）PLC 设备的供电（供电电能表的安装，电力线供电设备的安装次序等）。

2）确保实施对电力网络及其控制设备无影响的操作。

3）尽可能地识别出社区电力设施中电力网络上已有的低吞吐量的 PLC 网络，确认它们的位置（变电站、输电塔等）。

4）尽可能地确保社区 PLC 网络与已有的家庭或企业 PLC 网络能够互相兼容。PLC 网络之间以及不同 PLC 技术之间的共存问题将在第 13 章中予以阐述（该章将主要介绍混合网络）。

12.2.5　选择设备和技术

为一个社区网络选配 PLC 设备尤为重要，这是因为在主从结构的网络中需要使用一个与其他技术不相同的 PLC 技术。

Opera 联盟的项目中一个 PLC 的标准都没研究出来。鉴于截止到 2008 年 6 月 HomePlug 联盟还没有完成与 PLC 社区网络密切相关的 HomePlugbpl（标准），因此社区网络中的 PLC 技术的标准往往与每一个设备制造商都有关，即便是他们使用了 HomePlug 作为基础研究出供社区网络配电上使用的 PLC 设备，他们各自的标准也不尽相同。

因此将不同技术的标准（满足公共电力网络上的主从结构需要的）进行对比是非常重要的。出于这个目的，表 12.2 总结了配电网络上各种 PLC 技术的优缺点。

表 12.2　使用 PLC 技术的配电网络的优缺点

技术	设备和功能	优　点	缺　点
Main. net	CuPLUS master CuPLUS repeater NtPLUS slave	大量 PLC 工程中已经明确的技术 PLC 信号的优良范围 监督工具（NmPLUS）	技术有些过时
Spidcom	Headend master Repeater CPE slave	可行的先进配置（开槽、功率谱密度等） 强大的工程支持 SpiDM 管理监测技术 通过 PHY 层的速率为 224Mbit/s	在法国部署少 管理复杂
DS2	HE master Slave of the apartment building type HG Slave of the CPE apartment type	公共网的稳定性 HTTP 简单的管理接口 用于管理/监督的 OMSPLC 工具 产品由 Corinex 供应商集成	与 HomePlug 产品不兼容
Ascom	Master Slave	简单的 Telnet 界面 简单的软件升级	低吞吐量 过时的技术

表 12.2 仅是一种示意性的分析，但是它可以为设计者选配最适合社区标准的PLC 技术提供有益的参考。

12.2.6 PLC 配电网络的监管

和企业 PLC 网络一样，PLC 配电网络需要一个监管系统来监测各类基础设施。PLC 配电网络的结构包含以下部分：

PLC 配电网络包含若干处于主-从模式的 PLC 设备以及直到最终用户的公共电力网络。

PLC 配电网络与 IP 架构的网络之间的连接（通过 Peering 协议），或 PLC 配电网络与因特网直接连接（通过因特网提供商）。

NOC（网络操作中心）。在这里中控计算机分成若干个组，监管不同的 PLC 配电网络。它们用来检查网络中 PLC 设备的工作状态，主要采用的手段就是利用 GPS 地图成像功能从而确定各个设备的相对位置。

图 12.12 示意性地给出了一个 PLC 配电网络的例子，在这个例子中使用了 VPN 通道将 NOC 与 PLC 网关相连（网关位于电力变电站一端），从而实现对网络头设备的监管。

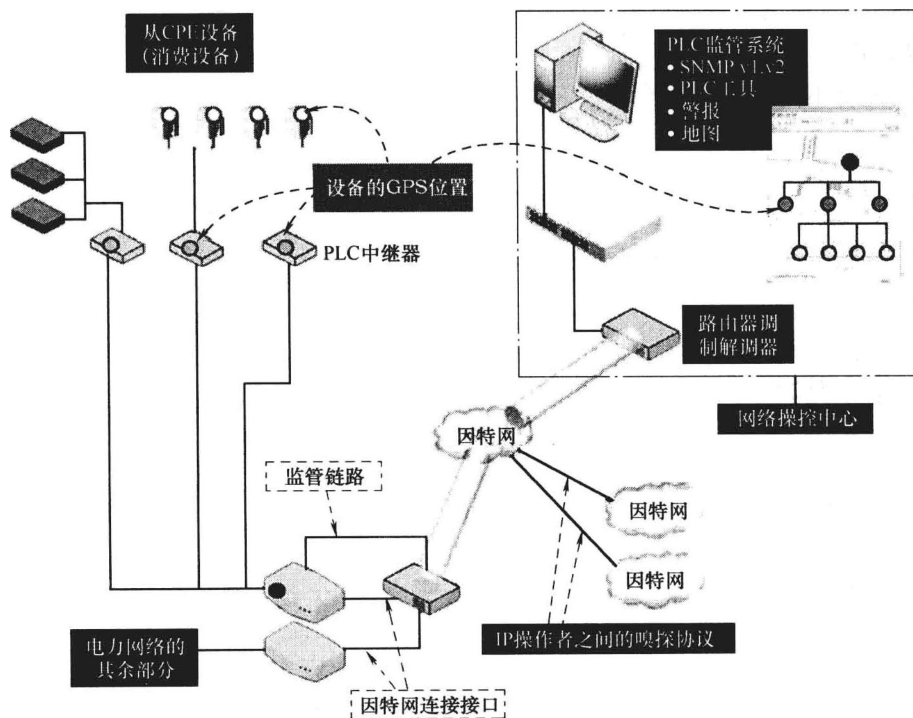


图 12.12 PLC 配电网络的监管结构

在这个结构中所有设备都可以通过 SNMP 或者 TR-096 协议来实现监管，即用有关的工具获得反馈信息（吞吐量、接口状态、温度、二进制误码率等）以及触发门限警报。

为了清晰地获得网络设备的 PLC 参数就必须使用与每一个所应用技术相匹配的工具。举一个例子：DS2 的产品就配有 OMS-PLC 工具，该工具是由 DYNAMIC CONSULTING INTERNATIONAL 公司专为管理 DS2 配电网络技术而开发的。

12.2.7 网络配置

我们可以看到，很多不同的技术都可构建 PLC 配电网络，根据不同结构的需求选择最合适的技术就成为承包商的主要工作之一。

图 12.13 示意性地给出了完整的电力线配电网络结构，主要包括：

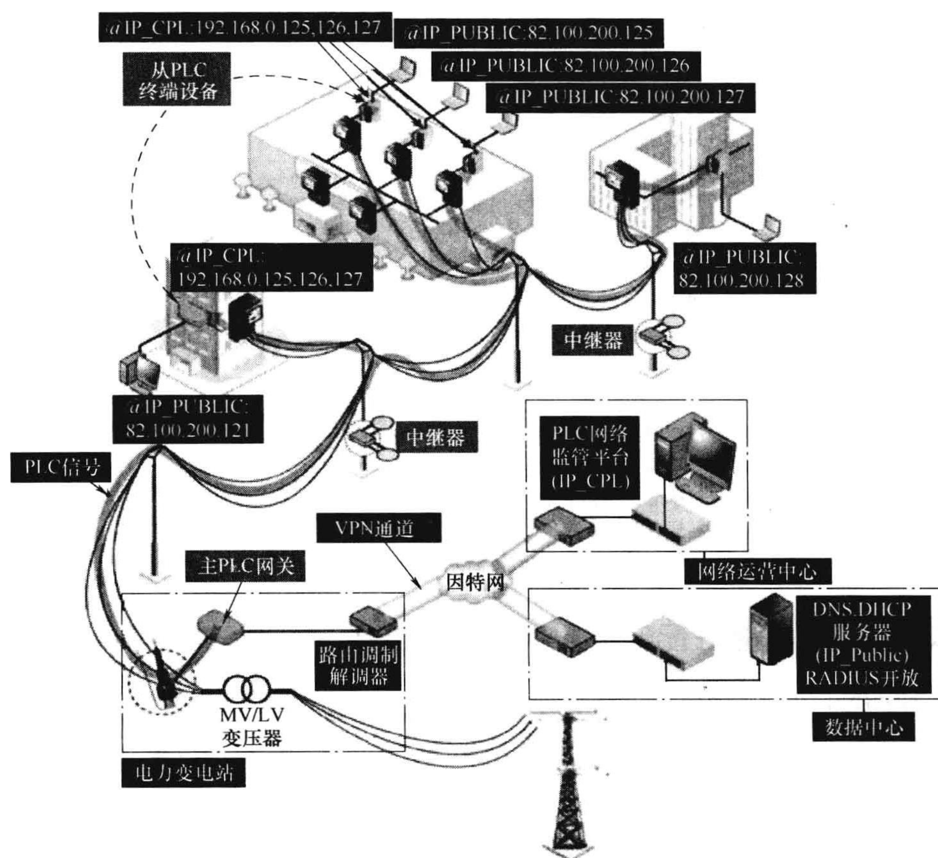


图 12.13 PLC 配电网络的示意图

1）连接至 PLC 网络的 IP 网络及其数据中心，它提供组验证、地址和名称服务。其 NOC 用于处理远程网络的监督和管理事宜，这一点和 PLC 配电网络是类似的。

2）PLC 配电网络，以及 PLC 主网关或者电力变电站处的网关（包括 MV/LV 变压器、中继器以及 PLC 从 CPE 设备）。从设备连接到主设备上，可以通过 IP 地址对其进行访问，这个 IP 是内部 IP 而不是连接到公共因特网上的 IP。

3）PLC 注入器。这个注入器用来将 PLC 设备连接到低压或者中压公共电力网络上，它的位置一般在电力变电站或者在靠近最终用户的电塔上。

显然，我们不可能将每一种技术的配置情况一一分析，因此我们仅仅分析一下每种配电网络重要技术参数的配置情况，见表 12.3。

表 12.3 配电网络中每一种 PLC 结构需要设置的参数

设备类型	需要配置的参数
主设备	因特网连接参数 授权的从设备列表 MAC 地址及 IP 地址过滤器 从设备之间的机密安全性 认证服务器的配置（如 RADIUS，PPP 等） 用于管理接口的 NAT 以及防火墙
中继器	PLC 网络组成的分割情况表 PLC 网络密钥 物理或逻辑上的复原能力
从设备	PLC 网络密钥 与主设备相关的认证 用于管理或监督的 IP PLC 寻址 品质（QoS）管理或者 IP 服务分级（如语音、数据、视频）

12.2.8 PLC 设备在配电网络中的 GPS 定位

为了优化对电力网络中设备的监督和管理以及维护与干预程度，电力网络中的每个设备都可以使用 GPS[⊖]来进行定位。这个 GPS 定位功能也可以很方便地用在网络操作中心（NOC）监管软件提供的结构图上，清晰地标注出每个结构组件的位置。

⊖ 这里的 GPS 并不是指全球卫星定位系统，而是指类似定位系统那样明确系统中各个组成部分的位置。这是作者法语原文中固有的幽默和会意，翻译过程中，译者予以保留这一用意。——译者注

已经有一些产品可以通过电力网络的主设备的 HTTP 接口来实现对每一个设备的位置进行配置，如图 12.14 所示。

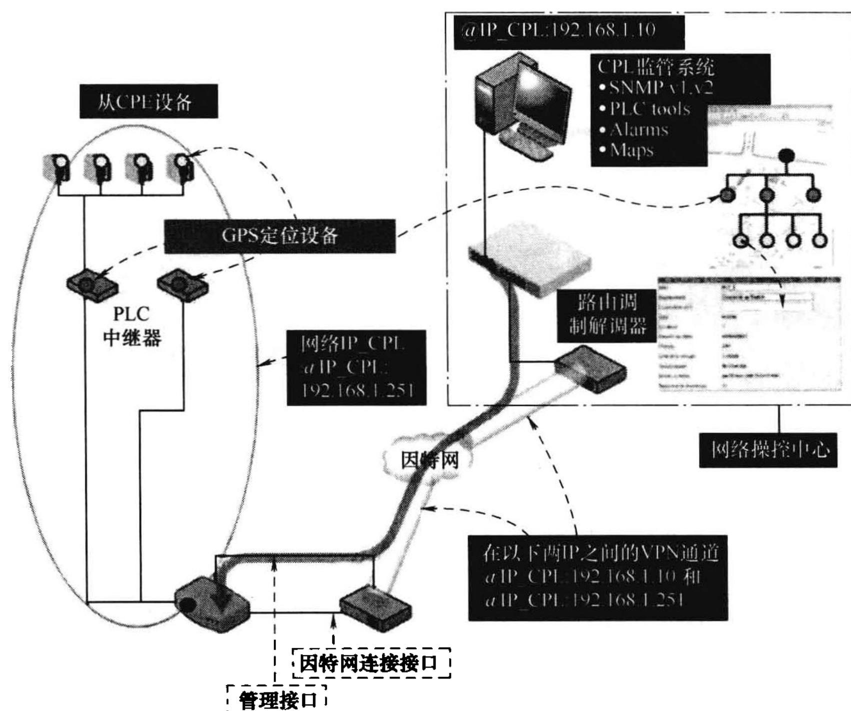


图 12.14　配电网络设备定位配置 PLC 结构图

为了实现这一目的，就需要将 NOC 和 PLC 架构中的设备与这类产品的 HTTP 配置通过 VPN 通道相连接，这样 NOC 与 PLC 网络位于同一 IP 地址段内。例如在图 12.14 中，监督台的 IP 地址是 192.168.1.10，PLC 网络的 IP 地址是 192.168.1.251。

一旦通过接口建立了连接，就可以从图 12.15 所示的目录按钮下的地址源目录中选择需要的设备（从设备或中继器，这些设备通过接口层的 MAC 地址来识别）。

12.2.9　小型、中型以及大型 PLC 网络举例

近年来，人们已经尝试在社区电力网络上使用 PLC 系统并进行了一些实验。

这些实践使得运营商的研究与开发可以在实际网络条件下以及用户层面进行实验。很多小区有着不同的运营商、不同的电力设施，这些小区都已经在准备着首次通过 PLC 提供国际因特网的接入。

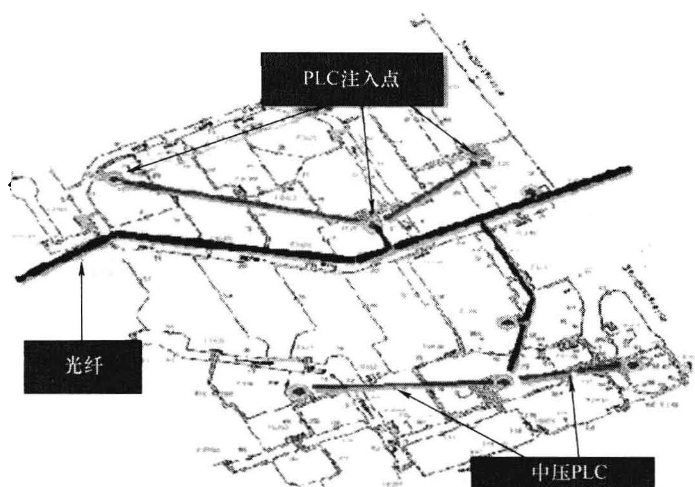


图 12.15 APPCPLC 应用结构（来源：CIGRE）

在其他一些更为领先的国家中，诸如美国、西班牙、瑞士等已经在整个城市中使用了 PLC 网络。最近，中国的一些光纤运营商也为新建筑物中成千上万的人们开发了 PLC 网络。

近来一些情况表明，对于一些主要的因特网弄潮儿而言，PLC 网络代表了具有发展潜力的分布式技术。

12.2.10 小型的 PLC 网络

根据其任务，EDF 研究和开发部门 2002 年在 Courbevoie 公社（法国）中开发了一款 PLC 配电网络，这款 PLC 配电网络得到了 Tiscali 因特网提供商的因特网连接支持。

这个配电网络旨在检测位于密集城市环境下的 EDF 低压配电网络的因特网接入的质量（采用星形电力网络拓扑树）。

这个网络包括了一根提供连接因特网并提供高吞吐量的光纤，并将其连接到向 100～200 个 EDF 用户供电的本地电力变电站。

在电力变电站，PLC 设备用于向自变压器开始的电力线中注入 PLC 信号，以及向不同的本地建筑物的房间提供服务。这些电力变电站处的 PLC 设备是主设备。

PLC 从设备经由各个房间连接到 PLC 网络中。它们都拥有合适的逻辑认证机制，从而能够继续使用来自 Tiscali 因特网提供商的因特网信号。这一提供商管理用户的认证事宜，并且向每一个 PLC 配电网络中的用户分配 IP 地址。

12.2.11 中型的 PLC 网络

根据缩减数字鸿沟的政策，特别是对郊区环境下高吞吐量因特网接入的关注，

Seine-et-Marne 地方议会（法国）已经在 Villeneuve-Saint-Denis 以及 Villeneuve-le-Comte 公社应用了卫星、PLC、Wi-Fi 网络技术等。

应用 PLC 配电网络使得那些 ADSL 无法服务的“空白”地区可以享有高吞吐率的网络连接。因此这两个公社可以通过靠近这两个公社的接入点，通过一个完整的 PLC 结构来实现高吞吐率的因特网连接。

12.2.12　大型的 PLC 网络

除了法国，大型的 PLC 配电网络已经在西班牙（Saragossa 以及巴塞罗那）通过 DS2 公司付诸实现；在美国，Current Technologies 公司在马里兰州和德克萨斯州应用了 PLC 网络，该网络可为 200 万人提供 4Mbit/s 的对称因特网接入。

Fribourg（瑞士）是首批应用 PLC 配电网络的城市之一，在 2001 年基于 Swisscom 因特网接入提供商，由 Ascom 技术公司设计实施。

在法国主要的 PLC 配电网络项目之一是由 Sipperece 公司资助的，这是一个 Ile-de-France 部门的能源和通信领域的集团公司。

12.2.13　PLC 网络应用的例子

表 12.4 给出了全球范围内正在和已经开发的 PLC 应用情况。

表 12.4　世界大型 PLC 网络部署实例

部署区域	部署国家	PLC 公司	注　释
美洲	美国	Amperion	Cap Girardeau, MO
	美国	Current Technologies	HomePlug1.0 Turbo, AV technology
	巴西	Light	低传输速率应用
欧洲	德国	EnBW	在埃尔旺根地区 ASCOM 技术
	西班牙	Iberdrola	基于 DS2 技术
	丹麦	PowerNet	Wi-Fi 的补充
	法国	TLIC	基于 MECELEC 网络技术
	德国	PPC	Main.net 技术
	西班牙	Epresa	远程服务技术
	西班牙	Endesa	基于 DS2 技术
	俄罗斯（莫斯科，诺夫哥罗德和克拉斯诺达尔）	Electro-com	为 35000 用户提供宽带因特网接入，电话和电视服务
	匈牙利	23Vnet	对 100 多用户进行高速宽带测试
非洲	尼日尔	Electrical operators	在几个城市测试
	阿尔及利亚	Sonelgas	在学校、大学和医院测试
	埃及（亚历山德里亚，法耶德，坦达）	Engineering Office for Integrated Projects, Corinex	7 万用户自动抄表
	南非（比勒陀利亚）	因特网接入方案	为 5000 用户提供宽带因特网接入

（续）

部署区域	部 署 国 家	PLC 公司	注　释
亚洲	中国	FibrLink	5 万测试用户
	日本	Panasonic	NTT Docomo 室内应用

在欧洲另一个应用的实例是位于德国的 PPC 公司。

在德国大约有 10000 名终端用户正在使用基于 LV-PLC 的商业网络服务其中，85% 的最终用户使用的 PLC 服务由 Power Plus Communications AG（PPC）公司提供。这一技术是基于 Main. Net 有限责任公司（以色列）的 PLC 系统。PPC 公司是 PLC 系统集成商并且在 2005 年 3 月份在整个德国安装了（为一部分操作者）一些商用的和测试的设施（103MV PLC 连接）。

在德国中压电力线大多数情况下用于低压电力线网络变电站之间的骨干连接，它并不直接连接到光纤骨干网。

80% 的电力线用来作为已经安装的低压电力线系统的骨干网，20% 用来租给专业的工业用户。在这些线路中有 101 条线路已经实现了 PPC 不同类型设备的容性耦合能力。在两个测试系统中安装了 Eichhoff 公司的感应耦合器。

PPC 公司已经在相当数量的中压配电室内安装了 PLC 设备，中压室的电压各不相同，互相绝缘也不尽相同。电压变化的幅度为 6～30kV。图 12.16 给出了德国的一个典型的安装在有容性耦合器的空气绝缘（SF_6）室的中压 PLC 设备的情况。

图 12.17 给出了另一个容性耦合设备安装在中压室的情况。

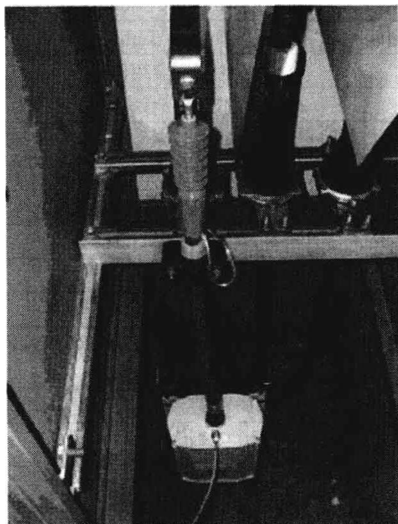


图 12.16　在一个空气绝缘的 MV 室中的容性耦合示例（来源：CIGRE）

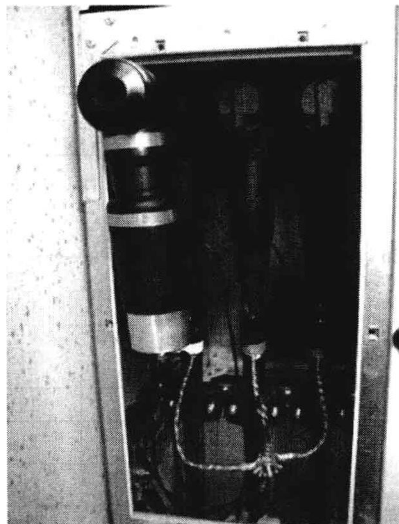


图 12.17　在一个气体绝缘的 MV 室中的容性耦合示意图（来源：CIGRE）

最大的吞吐速率是 3 ~ 5Mbit/s，这取决于德国 PPC 公司应用的线路条件。

在美国典型的例子便是 Current Technologies 公司。

2006 年底，该公司开发出了一个带有 TXU 的 BPL 系统，旨在为 200 万可能的用户提供传输速率为对称的 4Mbit/s 的基于 VoIP 的服务（45 欧元），如图 12.18。

安装在电线塔上的设备为基于 HomePlug（1.0 或 Turbo）的产品。CurrentTechnologies 公司使用的这个品牌的 HomePlug 产品为 AsokaUSA。

这一设备能够很好地适用于容性耦合器件、断路器以及熔断器。

至于我们关心的 BPL 网关，它包括一个同轴输入电缆（或光纤），并且具有路由功能（VoIP 数据流的 QoS + 认证 [IP 过滤器] + PLC 网关）。

HomePlug Turbo 允许一定数量的键值（最多 24），这样一来就可以构建一定数量的 PLC 逻辑网络。

Current Technologies 公司研发了物理层上的中继放大器用来对 MV 和 LV 线路上的 PLC 信号进行放大免致损失带宽，就像在 MAC 层上的 PLC 中继器一样。

Current Technologies 公司打算通过 PLC 接入因特网并使用以下配置：

1）卧室：IP 照相机的 IP 数据流从一个房间传到另一个房间。

2）起居室：来自视频服务器上的 MPEG-4 数据流（Windows Media9 ~ 1.5Mbit/s 解码器）。

3）办公室：PC + IP 打印机 + 交换机 + 用户 PLC 设备。

Current Technologies 公司设计了一套系统。这些信息与网络上的各种电力参数（如 kVA、kWh、漏电电流等）有关。通过 HTTPS 中央接口，利用有关工具就可以得到这些参数。

这个接口用来呈现以下信息：

1）变压器（变压器负载、历史报告等）；

2）电能表（历史报告、电压、默认值等）。

接口可以与 GIS（地理信息系统）一起工作，这样一来，变压器和电能表的数据就可以在有疑问地区的地图上直观地显示出来。同样地，这个接口可以通过电能表以及其他测量仪表反馈回来的报警信息来判定电力网络的故障。

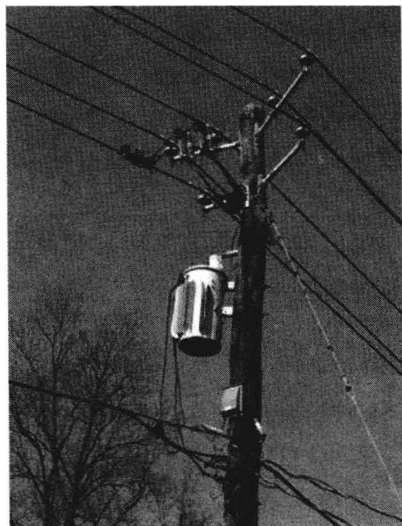


图 12.18　安装在输电塔上的 Current PLC 网关（来源：Michel Goldberg）

对 Current Technologies 公司而言，PLC/BPL 不是其核心业务。该公司宣称其经济策略在于 BPL 可以赢得收入，从而确保其 AMR 业务的开展（指自动抄表系统以及“智能电网”）。

第 13 章　混合 PLC

计算机通信媒介近来的进步（有线以太网、Wi-Fi、PLC、光纤、电视电缆等）使得网络媒体得以成倍地发展，为新一代的应用提供了合适的吞吐量，覆盖以及传输时间上的支持。

显然，各种媒介技术自己所能提供的网络容量是有限的，因此，为了能够最优地使用这个技术，就势必要使用混合网络技术。进一步讲，为了优化技术结构和配置，就必须对各种网络新技术有深入的了解。

目前，有线以太网因为它与有线网络是相关的，因而成本也是最贵的，但是它却是一种能提供最佳性能，满意服务率接近 100% 的技术。当不能构建这种网络的时候，就可以转而使用其他弥补的手段。

本章将着重分析 PLC 与其他技术的优劣。随着 HomePlug AV 标准的出现，PLC 技术便更多地呈现出它的优点（安装简便、成本低、终端开放以及安全等），以及与技术相比所呈现的优势。

13.1　多网络共存

多种网络技术共存时，不论是有线网络还是无线网络，均会产生干扰。例如，PLC 信号在电力线中传输时，会激发电磁场，这个电磁场可能会对其他通信系统（例如无线电通信系统）产生干扰，也可能对在各 PLC 系统自己产生干扰。

既然研究多种网络技术共存的目的就是确保 PLC 与 Wi-Fi 的共存。因此，了解并控制这些干扰显得尤为重要。

13.1.1　各种 PLC 技术

阅读了本书之后，我们已经发现，IEEE 关于 PLC 的有关标准尚未建立。因此，多种 PLC 技术就在公共或私人电力网络处于共存状态。

图 13.1 表明，在一个建筑物中，就有 3 种不同的 PLC 技术共同应用，它们分别为：

1）用来接入因特网的 PLC 群体的配线；

2）将视频数据流从因特网向分散在建筑物内的视频终端附近的 PLC 设备传输的线路；

3）用以建筑物内 IP 电话广播、建筑物自动数据发送系统（遥控、传感器信息等）以及本地信息（婴儿电话、视频监控等）的线路。

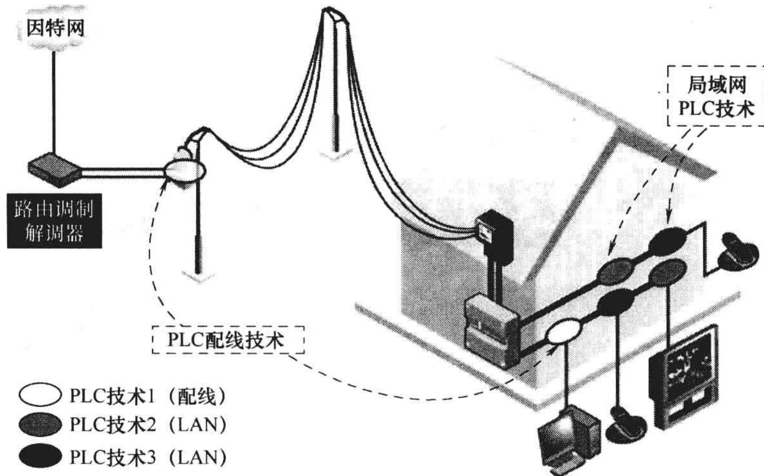


图 13.1　在相同电力网络中共存的 PLC 技术

上述 3 个 PLC 技术都是高数据吞吐量的应用，并且它们都工作在 2～30MHz 频段，不同的是，它们使用不同的技术接入到媒介中，且使用的频率各不相同。显然，如果没有一个互操作性的标准，这些技术将不可能朝着共存的方向发展。

CECPA 正致力研究 PLC 技术之间共存发展的基本原则，从而确保最优的频率应用。

13.1.2　CEPCA 以及 PLC 技术的互操作性

为了 PLC 标准，CEPCA 起草了一个技术建议，旨在研究 PLC 技术的共存。这个建议是基于公共分布式功能协调（Commonly Distributed Coordination Function, CDCF）方式基础上的。CDCF 方式旨在为不同的技术使用分布式的方法协调频率和时间。

分配协调方式基于以下几个方面：

1）FDMA 和 TDMA 之间混合接入控制；

2）TDMA 时空系统 QoS 控制，如供高清晰视频应用的 HomePlug AV。

图 13.2 给出了避免人为互相干扰，优化公用通信媒介使用的两个基本原则。

PLC 技术共存主要的问题源于频率使用得不标准，结果导致每一种 PLC 技

术的可用带宽减少。虽然数据通信是可以实现的，不过通信质量降低，甚至相当低，影响了为上层（IP、TCP 等）提供的路由传输，最终影响了应用的可操作性。

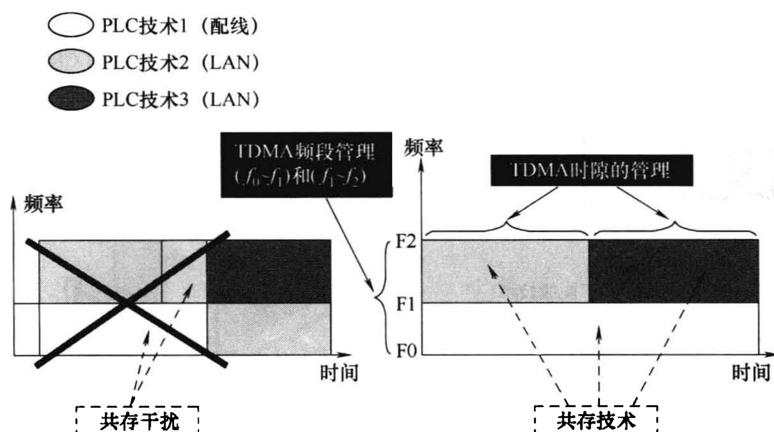


图 13.2 关于 PLC 技术之间的共存干扰解决方案的建议

我们应该避免在同一个电力网络中使用过多的 PLC 设备（例如 HomePlug1.0 和 Turbo 中，最多使用 16 个设备）。同样地，对在 HomePlug、DS2、Spidcom 等电力网络中，也必须努力避免在同一个电力网络中使用不同的 PLC 技术。

CEPCA 的建议与 HomePlug AV 近似，都是在为 HomePlug1.0，Turbo 以及 AV 网络提供基于 TDMA 的时空分配序列，见本书第 3 章和第 5 章。

图 13.3 形象地展示了共存条件下的系统。一些时隙分配给 HomePlug1.0 设备用作数据交换，另一些时隙用于与其他 HomePlug 标准进行数据交换。

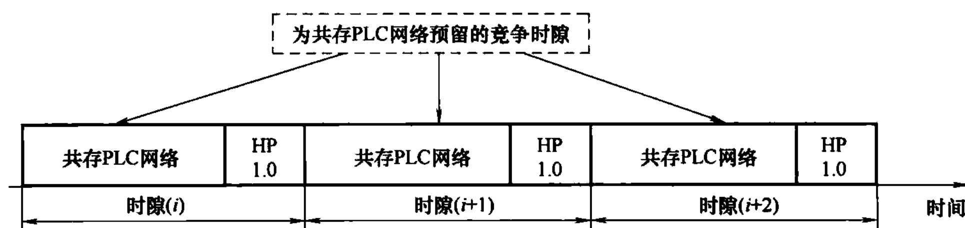


图 13.3 HomePlug PLC 网络与 HomePlug AV 标准之间的共存管理

这种为众多 HomePlug 技术提供设备共存的智能管理方法应当推广到其他的系统之间的共存中去，并有望研究出一个 IEEE 标准。

如表 13.1 所示，大量 HomePlug 标准的研制都致力于互操作性以及 PLC 终端

的开放性。与此相对应，其他的 PLC 技术既不与 HomePlug 互通，其相互之间也不相通，这就限制了这些 PLC 网络的开放性。

表 13.1　PLC 技术之间的互操作性

PLC 技术 A		PLC 技术 B						
		HomePlug					DS2	Spidcom
		1.0 Turbo	AV	Oxance	BPL	CC		
HomePlug	1.0 Turbo							
	AV							
	Oxance							
	BPL							
	CC							
DS2 AV200								
Spidcom								

13.1.3　PLC 和 Wi-Fi 的共存

因为所使用的频段不同，PLC 和 Wi-Fi 之间的共存不存在问题。PLC 使用 1～30MHz 频段，大量的 IEEE 802.11 标准的技术则使用 2.4GHz 和 5GHz 频段。

在结构方面，两者的共存不存在问题，这就使得两种技术都可以发挥较好的作用。于是，很多 PLC/Wi-Fi 设备就应当适用以 PLC 为骨干网，以 Wi-Fi 技术为基础的分布式 IP 网络的混合网络。

Lite-On 公司已经宣布，近期已经推出了一款类似天花板上照明灯泡式样的 PLC/Wi-Fi 设备。通过电力网，使用该设备可以传输 PLC 信号，提供 PLC 的相关功能，同时这个灯泡一样的设备也提供 Wi-Fi 接入的功能。

在房间的天花板上建立 Wi-Fi 接入点是优化房间覆盖的理想做法。

如图 13.4 所展示的就是一个 PLC/Wi-Fi 混合设备的例子，在图中可以看出，网络连接到 PLC 网关上，通过电力网络广播 PLC 信号。这些信号通过 PLC/Wi-Fi 设备的 IEEE 802.11 无线接口建立在众多房间中的 Wi-Fi 覆盖单元。

下面以 Zyxel 公司的 NBG318S 设备为例，如图 13.5 所示，分析这种混合结构的配置。

Zyxel 公司的设备包含适用于以太网 PLC 接口的路由器，以及一个带有插座的 Wi-Fi 接口和基于 IEEE 802.11 标准的天线。

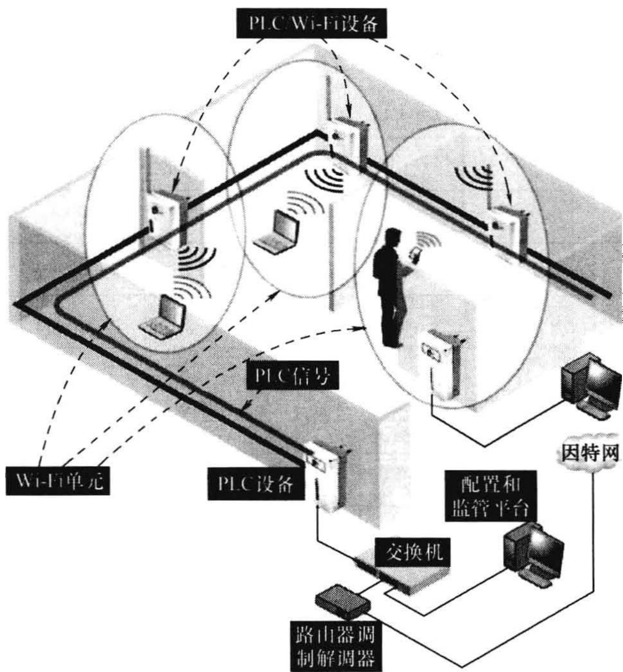


图 13.4 PLC/Wi-Fi 混合结构的示例

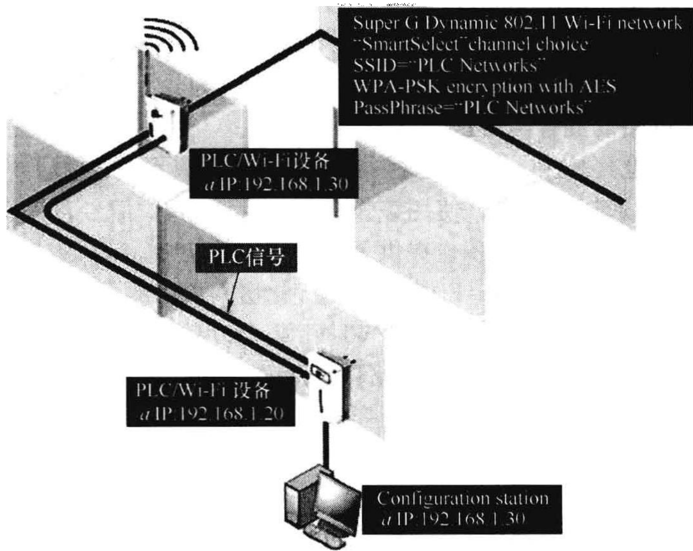


图 13.5 PLC/Wi-Fi 设备的配置

这种混合网络的配置要求设置 Wi-Fi 设备的参数。如图 13.6 所示，这些参数经由通过一个 HTTP 接口在 Wi-Fi 设备一端来配置。

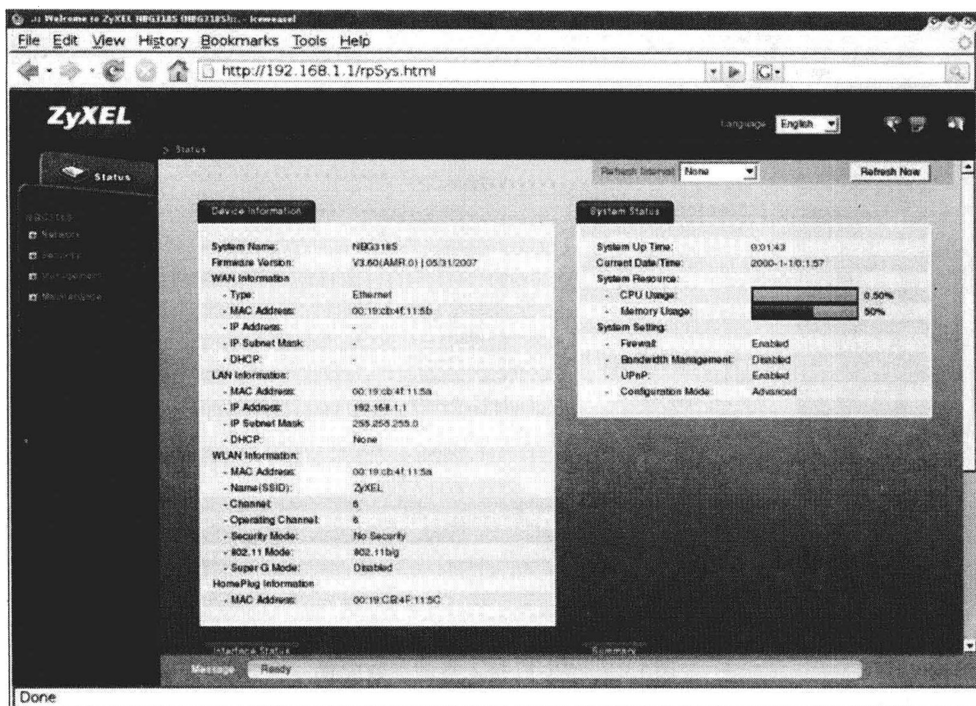


图 13.6　连接到作为 Wi-Fi 接入点的 PLC 设备上

网络管理台式机的地址设置为 192.168.1.2，PLC/Wi-Fi 设备的默认地址设置为 192.168.1.1。下面你需要做的就是将以太网管理台式机连接到 PLC 设备上，然后在 Internet Explorer 浏览器中打开 192.168.1.1 地址。

这时候就会出现图 13.6 所示的窗口，默认密码是 1234。

建立上述连接后，就可以通过图 13.6 所示的界面显示 Wi-Fi 接入点的默认参数，这个接入点的安全性必须予以设置。

在网络菜单的 WLAN 子菜单中，改变管理接口操作权限的用户名和密码是很重要的，因为这是为了避免其他人连接到 PLC 网络实行 Wi-Fi 网络的配置。

下一步配置是 Wi-Fi 网络的其他参数以及设置安全性。首先，必须选择一个 SSID（也就是 Wi-Fi 网络名），这样用户才能连接到这里。PLC 网络的选择如图 13.7 所示。

然后，可以选择 2.4GHz 频段的一个信道（从 1～13）。

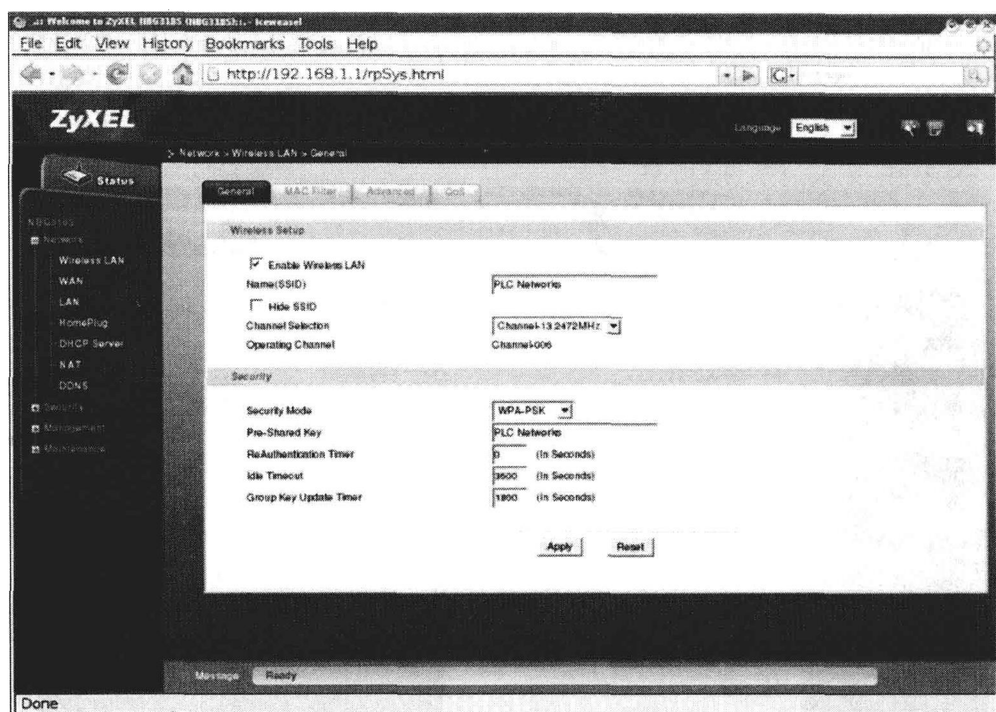


图 13.7 Wi-Fi 接入点的参数配置

选择 IEEE 802.11 的模式

如果网络选择了“IEEE 802.11 超级 G 动态模式”，那么就要确保所有接入网络的 IEEE 802.11 用户都支持这个模式。如果不是这种情况，则应选择被大多数 Wi-Fi 终端支持的 IEEE 802.11b 或 IEEE 802.11g 模式。一旦 IEEE 802.11 网络模式确定，我们就可以进行 Wi-Fi 网络安全的参数化，这是 Wi-Fi 网络的一个弱点。

目前为止，PLC 网络是安全的，并且本身不容易被接入，因此对整个混合网络而言，就可以确保一个理想的安全级别。例如在前面的例子中，系统配置菜单的无线安全子菜单用来选择 WPA-PSK 模式，通过加密短语以 AES 密钥来加密（然而，通常说来，这一加密方式必须被 Wi-Fi 用户支持）。

Wi-Fi 网络的整个配置已经完成。我们接下来配置 PLC 网络以及其参数。如图 13.8所示，网络菜单的 HomePlug 子菜单用来完成接入 HomePlug AV PLC 参数的配置。比如说，在子菜单中可以将网络名称选项卡中的网络类型选择为“公共（Public）”，即保持 HomePlug AV 的默认设置不变；也可以选择“私人（Private）”，并为这个包含该设备和电力网络中的其他 PLC 设备的 PLC 逻辑网络配置一个新的

NEK 键值。从而实现将这个网络的名称设置为公开（保持 Homeplug AV 默认值不变）或者私人。

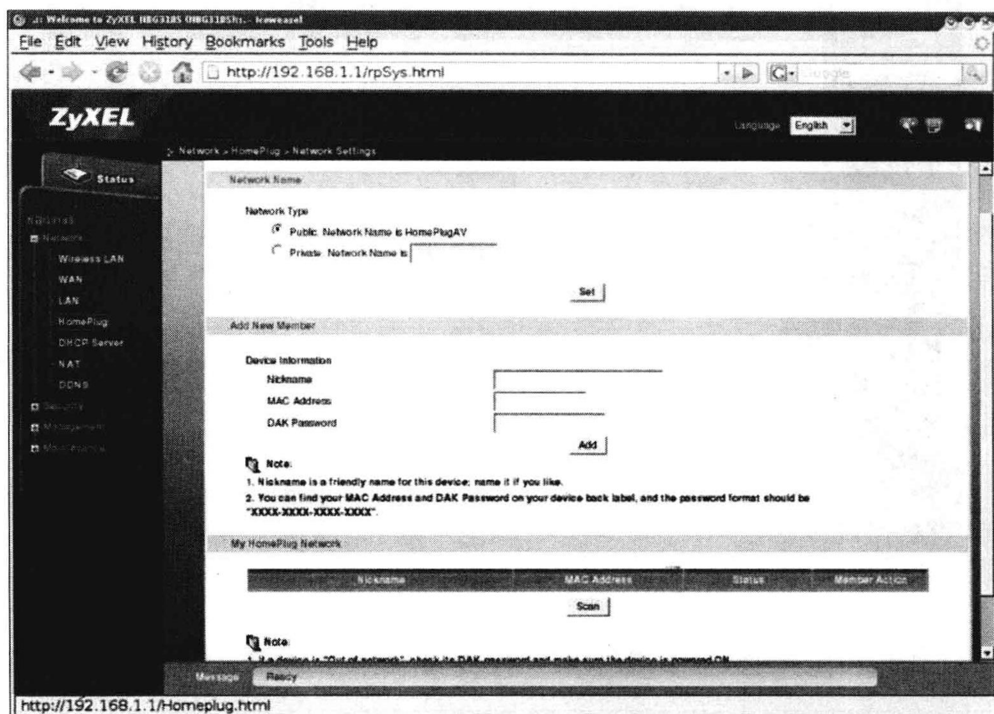


图 13.8 为 HomePlug AV PLC 网络配置参数

从不同设备的 MAC 地址来讲，为了有一个更好的可读性，就需要对网络中的 PLC 设备进行命名。相关联的 PLC 设备的默认命名可以为“Example 1”。这种情况下，关联相关的设备后，如果我们将图 13.8 所示的 HTML 页面刷新，就会看到如图 13.9 所示的关联后的结果。

当所有 PLC 设备与 HomePlug AV 网络关联后，就可以选择 Wi-Fi 和 PLC 接口之间的路由模式。这一接口扮演了与对方之间的网关的角色，就如同将两种技术桥接起来一样。

最后，用于连接到网关或者通过路由器接入另一个 IP 网的 WAN 接口可以按照图 13.10 所示的界面进行配置。

上述配置实例表明，PLC/Wi-Fi 混合网络结构所包含的组成部分可以进行简单快捷的网络配置，从而用电力网络作为以太网的骨干实现性能的最优化，以及用插座上的 PLC/Wi-Fi 设备作为分布系统实现无线电覆盖。

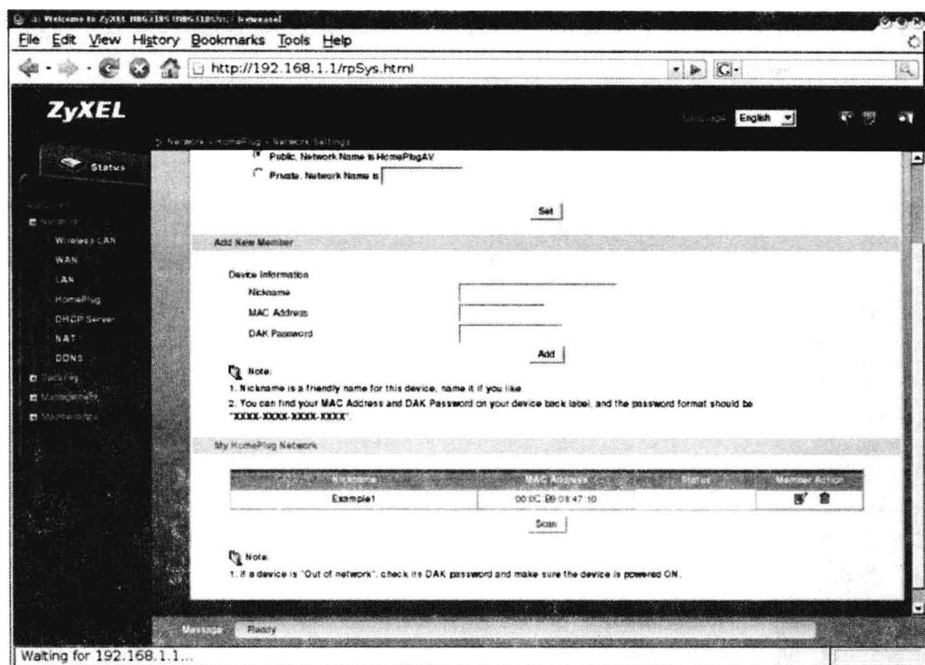


图 13.9 确认新的 PLC 设备关联到网络上

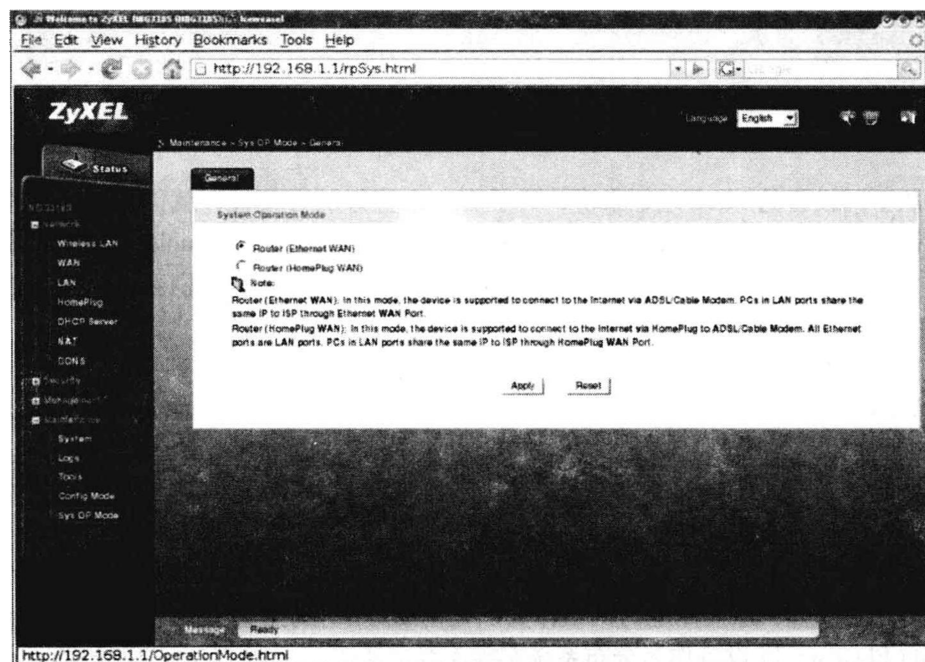


图 13.10 WAN 接口选择的配置

这样，PLC 和 Wi-Fi 的共存符合一般逻辑，又很自然地在家庭环境和专业环境下实现了通信的移动性。

13.1.4　PLC 和有线以太网的共存

PLC 和有线网络（以太线缆、光纤、线缆电视、电话线缆等）的共存不会产生干扰，因为其所用频段在 PLC 频段外。

只有 VDSL 分布式技术，它需要在铜电话线缆上实现约几十 Mbit/s 的接入吞吐量，并且它会使用 138kHz～12MHz 频段的频率。由于 PLC 技术在电线附近会产生在 2～30MHz 频段的电磁噪声，电平值可达 70～80dBμV（准峰值），因此 VSDL 可能会成为 PLC 潜在的干扰对象。

如图 13.11 给出了 VDSL 频带以及在这一频段上的 PLC 频带使用情况。

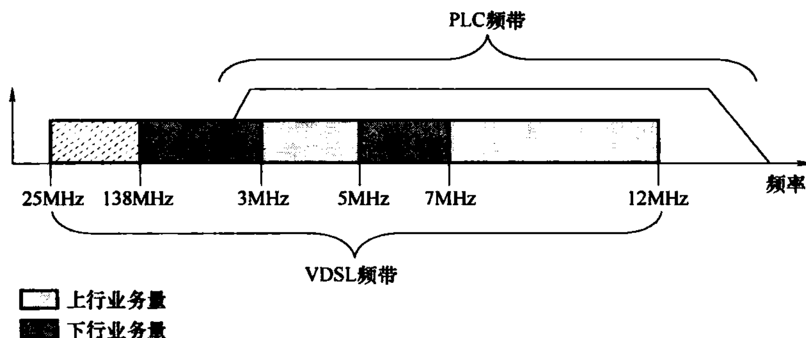


图 13.11　VDSL 与 PLC 频段中潜在的干扰

在局域网中，由于 PLC 和有线技术的共存不存在问题，因此，有线技术是 PLC 局域网的骨干技术。

13.2　网络技术的优点和缺点

为了比较 PLC 技术和其他网络技术，我们采取表 13.2 的形式总结每种技术的优点和缺点。

表 13.2　比较不同的网络结构

网络技术	成本	缺　点	优　点
以太网电缆 （CAT5 100BaseT）	高	布线槽 线缆成本	QoS 有保障 提高安全性（RJ-45 连接器接入控制过滤） 吞吐量保障 由 Poe 供电

（续）

网络技术	成本	缺　点	优　点
Wi-Fi (IEEE 802.11.g)	一般	无线电覆盖研究 WAP 和 AES 加密方式的实施 需要 RADIUS 服务 对 QoS 不能保证	网络开放性 移动性和切换 基于 Wi-Fi 的 ToIP 与有线骨干网混合
有线电视	布线开槽成本则高	布线开槽 需要授权后才能共享媒体	可以使用现有线缆 确保 QoS 很难接入到物理介质
光纤 (塑胶纤维)	高	布线开槽 有源设备成本	很高的吞吐量 抗噪声 是理想的有线骨干网 很难接入到物理介质
HomePlug Turbo PLC	一般	需要场地及电网络工程研究 需要对电网知识有较好了解 一些设备的接入存在困难	高的吞吐量 配置简单 网络开放 临时建网简单 媒介安全性好 在一个电网络中存在数个 VLAN
HomePlug AV PLC		需要对电力危害有了解	对 HD 视频应用提供好的吞吐量 确保 QoS 与其他 HomePlug1.0 和 Turbo 设备兼容 符合电磁抗干扰需求 组建 PLC/Wi-Fi 混合网络
电话线	如果布线开槽则高	公共电话网络归属法国国家电信	使用现有线路 高的并且有保证的吞吐量 确保 QoS 物理媒介安全性好

表中的一些技术得以大量应用，因为它们具有其他技术所没有的一些功能（例如价格、部署的难易、公开性以及安全性等）。

13.3 优化网络结构

为了能够最大限度地发挥现有各种网络技术的功能，需要寻找每种技术中的最优者以便组建一个最理想的网络架构。基于此，我们有必要分析将要建立的网络参数并且列举出建筑物的最重要的特征。

网络工程研究旨在特别明确以下几个方面的特性：

1）建筑结构（屋子大小、开槽的可能性、用于无线电传输的墙体材料等）；

2）已有网络（连接若干建筑物的个人电话网络、有线电视网络等）；

3）电力网络图和断路器面板的位置；
4）期待的网络性能（如传输时间、延迟、电网起伏等）；
5）开放性，可移动性，临时网络，测试网络等；
6）用户组和特殊逻辑网的要求；
7）网络部署、配置以及整体监管的难易。

构建一个网络结构需要明确上述各方面特性，从而确保有效性和稳定性。

我们采用相同的方法，以表格的形式分析各种网络结构的最优化应用方式，见表 13.3。

表 13.3　网络技术的最佳应用条件

网络技术	最佳应用条件
以太网电缆	便于开槽布线（电缆升井、其他计划的工作、电力由 PoE 供应等） 最优网络结构（星形、环形、树形等）
Wi-Fi	有效无线电覆盖 较好的越区切换 较好的安全管理
有线电视	便于开槽布线 现成的物理介质
光纤	便于开槽布线 有源设备优化多路性 选择好光模式和波长
PLC	很好地了解电网 与有线骨干网混合的网络
电话线	在与 PABX 接近的地方安装设备 可实现点对点连接

13.3.1　优化结构实例

我们以两个建筑的计算机网络安装为例，这两个建筑物之间存在从当地的 PABX 连接过来的私人电话线路，并且这个线路将两个建筑物连接起来。

由于建筑物是多层的，因此需要在两个建筑的每个屋子里以及两个建筑物之间都实现用户的移动性。我们假设，输入电网是可操作的，并且允许外接出附加的线路，且网络设备的安装是较为方便的。

在安装 PLC 设备之前，如有可能应了解每层电网以及整个建筑物的电网的有关情况。

为了达到要求，并符合有关标准，图 13.12 给出了混合网络结构，主要包括：

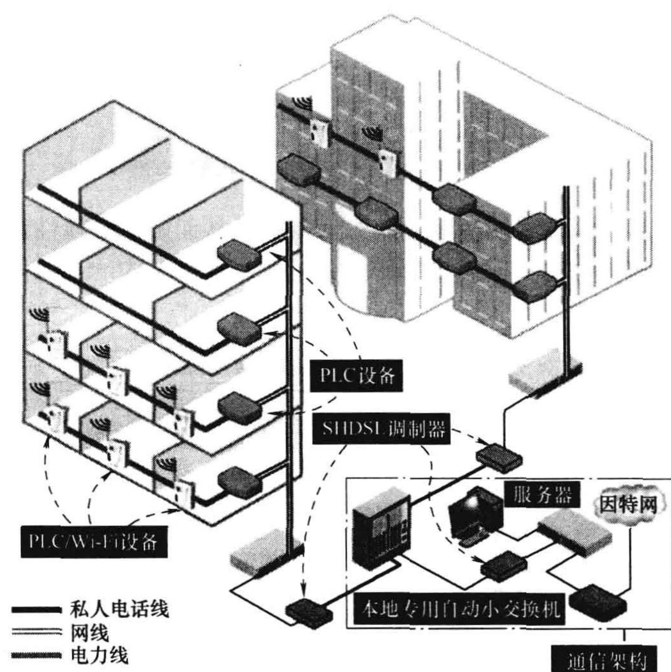


图 13.12 优化后的混合网络结构示例

1）在通信基础端和建筑物之间通过双绞电话线上的 SHDSL 调制解调器实现 IP 连接；

2）以太网骨干在电网升井处向每一层都提供 IP 连接；

3）PLC 的楼层网络通过网关设备连接到以太网骨干上；

4）PLC/Wi-Fi 混合设备在每一个房间插座上都有配备，实现 Wi-Fi 的完全覆盖；

5）用户连接网络时通过 IEEE 802.11 技术，或通过 PLC 设备连接到每层的 PLC 网关。

这个结构只是一个混合网络的示例。然而，它却最优地将每一网络安装到位，并且避开了安装位置的限制。当然，如果选择好合适的网络技术，那么这些所谓的位置限制就会转变为各个网络技术安装的优势位置。

13.3.2 PLC 和 Wi-Fi 的最佳组合

本书多次讲到，如果不考虑吞吐量、功能和设备成本的话，PLC 与 Wi-Fi 技术有很多相似之处。因此，人们自然就考虑到这两种技术紧密结合起来，作为以太骨干网，并且由 Wi-Fi 的接口提供本地客户的连接。

越来越多的制造商正在打算将两种技术融合到一个设备中去。近来的标准研究工作即将把融合了 HomePlug AV 技术 和 IEEE 802.11 超级 G 动态技术的设备投放市场，以求提供更高的吞吐量，为高清晰数据流媒体广播服务。

图 13.13 示意了 PLC 设备和 Wi-Fi 设备之间的帧交换，以及对应的一个 PLC/Wi-Fi 混合设备。设备制造商正在致力于在 PLC 和无线电接口之间的连接优化工作，从而免去帧的封包和解包环节。

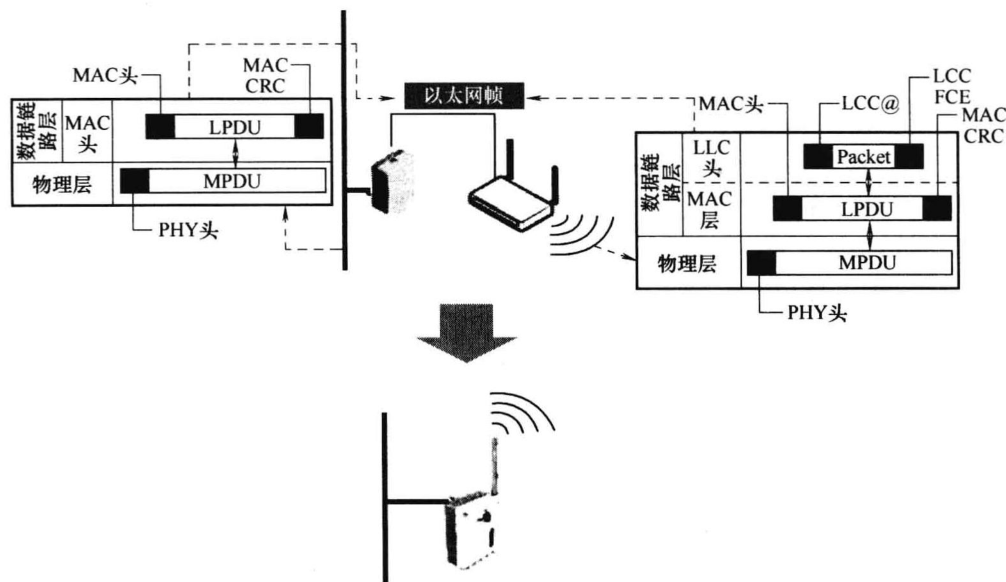


图 13.13　优化后的 PLC/Wi-Fi 设备

参考资料

有关网站

标准组织

IEEE：http://www.ieee.org

http://grouper.ieee.org/groups/1901/for the PLC network working group

ETSI：http://www.etsi.org

IETF：http://www.ietf.org

Cenélec：http://www.cenelec.org

IEC 及其 CISPR：http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=dirdet.p&progdb=db1&committee=CI&css_color=purple&number=CIS/I

PLC 技术

HomePlug：http://www.homeplug.org

DS2：http://www.ds2.es

Spidcom：http://www.spidcom.com

PLC 概要介绍

CPL News：http://www.cpl-news.com

Powerline Communications：http://powerlinecommunications.net

PUA：http://pua-plc.com

PLC Forum：http://www.plcforum.org

CEPCA Alliance：http://www.cepca.org

产品

http://www.aceex.com

http://www.acer.com

http://www.amigo.com.tw/

http://artimi.com/

http://asokausa.com/

http://www.atlantisland.it/

http://bewan.com
http://www.billion-france.com/
http://cometlabs.com/
http://www.courantmultimedia.fr
http://www.connectland.net/
http://www.corinex.com
http://www.defidev.com/
http://www.devolo.com
http://www.dynamode.co.uk/
http://www.edimax.com/
http://eichhoff.de
http://www.gigafast.com
http://www.ilevo.com
http://www.jaht.com/
http://www.leacom.fr
http://www.linksys.com
http://www.Main.net-plc.com/
http://global.mitsubishielectric.com/bu/plc/
http://www.msi-computer.fr/
http://netgear.com/
http://www.niroda.com/
http://www.olitec.fr/
http://www.ovislink.fr
http://www.packardbell.fr
http://peabird.com
http://phonex.com
http://www.powernetsys.com
http://www.powertec.com.au
http://www.sagem.com
http://www.schneider-electric.fr
http://siemens.com
http://smc.com
http://www.stt.com.tw
www.sei.co.jp
http://www.telkonet.com

http://www.omenex.com
http://www.xeline.com
http://www.xnet.com.tw
http://www.yakumo.de
http://www.zyxel.fr

低传输速率 PLC 技术

http://www.siconnect.com
http://www.itrancomm.com
http://www.arianecontrols.com

有关书籍和论文

DOSTERT (KLAUS), *Powerline Communications*, Prentice Hall, 2000

LEE (M.K.), NEWMAN (R.E.), LATCHMAN (H.A.), KATAR (S.), YONGE (L.), *Homeplug*1.0 *Powerline Communication LANs—Protocol Description and Performance Results*, *version* 5.4, 2000, Wiley.

PAVLIDOU (F.-N.), LATCHMAN (H.A.), HAN VINCK (A.J.), NEWMAN (R.E.), "Powerline communications and applications," *International Journal of Communication Systems*, 2003, Wiley.

HRASNICA (H.), HAIDINE (A.), LEHNERT (R.), *Broadband Powerline Communications: Network Design*, 2004, Wiley.